PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-232775
(43)Date of publication of application : 27.08.1999

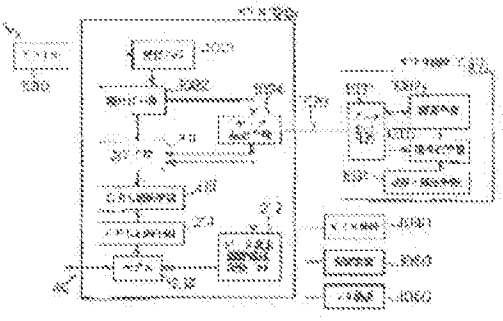
(51)Int.Cl. G11B 20/10

(21)Application number : 10-031646
(22)Date of filing : 13.02.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : YAMADA MASAZUMI
IIZUKA HIROYUKI
TAKECHI HIDEAKI
GOTO SHOICHI

(54) CONTROL STANDARD MAKING METHOD, CONTROL STANDARD MAKING SYSTEM, AND MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable detecting an illegal terminal device before damage occurs more surely than conventional one.
SOLUTION: When data is required from a VTR device 1030 and the like having respective intrinsic EU 164 to STB 120, a certification means 211 performs certification based on the prescribed control standard about their data request, it is decided whether required data is transferred from STB 120 to the VTR device 1030 performing request or not in accordance with the certification result, and a data request history information storing means 212 sends data request history information including EU 164 of the VTR device to a control device 110 in accordance with the certification result. The control device discriminates whether the VTR device 1030 is a regular one or not by the prescribed discrimination standard utilizing the data request history information, makes CRL based on the certification result, and sends it to the SBT 120.



(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－232775

(43)公開日　平成11年(1999)8月27日

(51)Int.Cl.⁶	識別記号	FI
G11B 20/10		G11B 20/10 H

審査請求　未請求　請求項の数13　OL　（全 15 頁）

(21)出願番号　特願平10－31840

(22)出願日　平成10年(1998)2月13日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　飯塚　隆之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

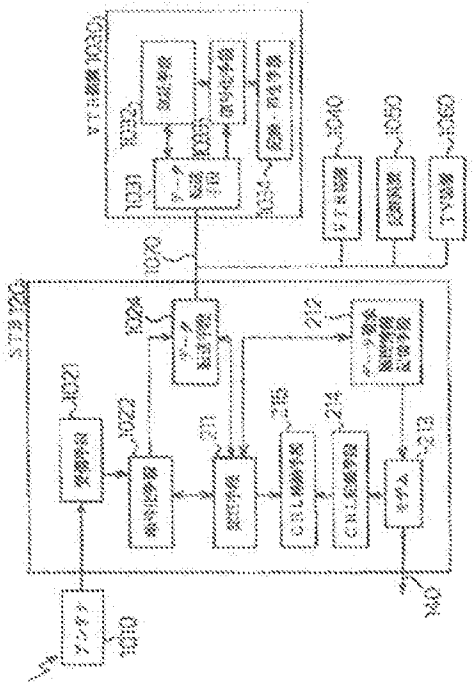
(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　松田　正道

最終頁に続く

(54)【発明の名称】　管理基準作成方法、管理基準作成システム、及び媒体

(57)【要約】
【課題】不正な端末装置を被害発生前に未然に検出できないという課題。
【解決手段】それぞれ固有のＥＵＩ６４を有するＶＴＲ装置１０３０等からＳＴＢ１２０に対しデータ要求があった際、認証手段２１１がそれらのデータ要求に対して、所定の管理基準に基づいた認証を行い、認証の結果に応じて、ＳＴＢ１２０から、要求を行ったＶＴＲ装置１０３０に対して、その要求された次データを転送するかどうかを決定し、データ要求履歴情報記憶手段２１３が認証の結果に応じて管理装置１１０に対して、そのＶＴＲ装置のＥＵＩ６４を含むデータ要求履歴情報を送り、管理装置１１０は、そのデータ要求履歴情報を利用して、所定の判定基準により、そのＶＴＲ装置１０３０が正規なものであるの否かを判定し、その判定結果に基づいてＣＲＬを作成し、ＳＢＴ１２０に送信する構成。



【特許請求の範囲】

【請求項1】 それぞれ固有の識別子を有する各データ要求端末装置からデータ転送装置に対しデータ要求があった際、それらのデータ要求に関して、所定の記録基準に基づいた登録を行い、

前記記録の結果にもとづいて、前記データ転送装置から、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定し、

又は、前記記録の結果にもとづいて、前記データ転送装置から定時的に、そのデータ要求端末装置の前記識別子を含むデータ要求記録情報を送り、

前記管理装置は、前記送られてくるデータ要求履歴情報を利用して、所定の判定基準により、そのデータ要求端末装置が将来に送信するデータ要求端末装置の妥当なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新することを特徴とする管理基準作成方法。

【請求項2】 前記複数のデータ要求端末装置と前記データ転送装置とにより形成されるグループは複数グループ有り、

前記データ要求履歴情報は、前記識別子の他に、その識別子を有する前記データ要求端末装置からの前記データ要求のあった時刻を特定する時刻情報と、そのデータ要求端末装置の存在を特定する所在情報とを含む情報であり、

前記管理装置における前記所定の判定基準は、前記複数のデータ転送装置から送信されてくる全てのデータ要求履歴情報の中で、同一の識別子が複数存在する場合、それら複数の識別子に対応する前記時刻情報及び前記所在情報をそれぞれ比較して、不正の可能性がある識別子を有するデータ要求端末装置を決定するものであることを特徴とする請求項1記載の管理基準作成方法。

【請求項3】 前記判定基準による判定結果、前記不正の可能性がある識別子を有するデータ要求端末装置が決定された場合、それら同一の識別子を有する全てのデータ要求端末装置を不正なものと見なし、前記管理基準として、それら不正なものと見なされたデータ要求端末装置の不正リストを作成、又は更新することを特徴とする請求項2記載の管理基準作成方法。

【請求項4】 前記管理装置は、前記不正リストの全部又は一部を前記データ転送装置に送信し、

前記データ転送装置は、前もって送信されてきた不正リストをメモリなくとも利用して前記識別を行うことを特徴とする請求項3記載の管理基準作成方法。

【請求項5】 それぞれ固有の識別子を有するデータ要求端末装置に接続されたデータ転送装置を単数又は複数管理する管理装置は、送られてくる、前後に接続される予定の又は新規に追加された前記データ要求端末装置の識別子を含む新規登録情報を利用して、所定の判定基準により、前記新規登録情報に対応するデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新することを特徴とする管理基準作成方法。

【請求項6】 前記複数のデータ要求端末装置と前記データ転送装置とにより形成されるグループは複数グループ有り、

前記データ転送装置は、予め記録された前記データ要求端末装置の前記データ転送装置との接続を検知した際、そのデータ要求端末装置の新規登録情報を前記管理装置に送信するものであり、

前記所定の判定基準は、前記新規登録情報が受信されてくる度に、その新規登録情報に含まれる識別子と同一の識別子が、前記複数のデータ転送装置から送信されてきて保持されている前記識別子のリストの中に、既に存在しているか否かを判定する基準でもあることを特徴とする請求項5記載の管理基準作成方法。

【請求項7】 前記判定基準による判定結果が、前記同一の識別子が前記リスト中に存在していることを示す場合、それら同一の識別子を有する全てのデータ要求端末装置を不正なものと見なし、前記管理基準として、それら不正なものと見なされたデータ要求端末装置の不正履歴を作成、又は更新することを特徴とする請求項6記載の管理基準作成方法。

【請求項8】 前記判定基準による判定結果が、（1）前記同一の識別子が前記リスト中に存在していることを示す場合、それら同一の識別子を有する全てのデータ要求端末装置を不正なものと見なし、前記管理基準として、それら不正なものと見なされたデータ要求端末装置の不正履歴を作成、又は更新し、又、（2）前記同一の識別子が前記リスト中に存在していないことを示す場合、前記新規登録情報に含まれる前記識別子を有するデータ要求端末装置を正規なものと見なし、前記管理基準として、その正規なものと見なされたデータ要求端末装置の正規情報を作成、又は更新することを特徴とする請求項6記載の管理基準作成方法。

【請求項9】 前記管理装置は、前記不正情報の全部又は一部を、又は前記正規情報を前記データ転送装置に送信し、

前記データ転送装置は、各データ要求端末装置からデータ要求があった際、それらのデータ要求に関して、前記送信されてきた不正情報又は正規情報をメモリなくとも利用して認証し、その認証結果に応じて、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定するものであることを特徴とする請求項8記載の管理基準作成方法。

【請求項10】 前記管理装置が、前記不正情報の一部を前記データ転送装置に送信する場合、前記不正情報に挙げられているデータ要求端末装置に関する情報のみ、そのデータ転送装置と接続関係にあるデータ要求端末装置に対応する情報を抽出し、送信することを特徴とする

請求項４又は５記載の管理基準作成方法。

【請求項１１】　それぞれ固有の識別子を有する複数のデータ要求端末装置と、

それらデータ要求端末装置からデータ要求が有った際、それらのデータ要求に関して、所定の認証処理に基づいた認証を行い、（１）その認証の結果に応じて、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定し、又、（２）更に、又はその認証の結果に応じて、そのデータ要求端末装置の前記識別子を含むデータ要求履歴情報を出力するデータ転送装置と、

前記出力された前記データ要求履歴情報を得て、所定の判定基準により、そのデータ要求履歴情報に含まれたデータ要求端末装置が正当なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新する管理装置と、を備えたことを特徴とする管理基準作成システム。

【請求項１２】　請求項１～１０の何れか一つに記載の各ステップの全部又は一部のステップをコンピュータに実行させるためのプログラムを記録したことを特徴とするコンピュータ読取り可能な記録媒体。

【請求項１３】　請求項１１に記載の各手段の全部又は一部の手段の機能をコンピュータに実行させるためのプログラムを記録したことを特徴とするコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、管理基準作成方法、管理基準作成システム、及び記録媒体に関する。

【０００２】

【従来の技術】従来より、衛星放送で送られてくるテレビ番組を、専用の受信機により受信して、その受信機に接続されたＶＴＲ装置で録画したり、テレビで視聴したりすることが行われている。

【０００３】この場合、伝送されてくる映像・音声データの中には、記録が禁止されているものや、１回だけ記録可能とされている条件付きデータがある。従って、これらの条件が守られる為には、この条件を正しく認識して、正規に動作する装置をユーザ側が使用することが前提となる。

【０００４】そこで、専用の受信機から、例えばＶＴＲ装置に対して、１回のみ記録可能なデータを送信する場合、先ず、そのＶＴＲ装置が、上記の様な正規な装置であるかどうかを確認するための認証動作が行われるのが通常である。この認証動作の結果、上記条件を無視した動作を行う不正装置であると判定した場合には、データの送信を行わないものである。

【０００５】以下、図１２を参照しながら、従来の専用受信機と端末装置との構成と、その認証動作を中心に説明する。

【０００６】図１２は、従来の専用受信機と端末装置との接続状態及び構成を示すブロック図である。

【０００７】同図に示す様に、アンテナ１０１０は、衛星からの伝送電波を受信する手段であり、衛星放送受信機（以下、これを単に、ＳＴＢと呼ぶ）１０２０は、受信した放送電波をＡＶデータに変換する手段である。データ伝送ライン１０７０は、ＳＴＢ１０２０と、以下に述べる各端末装置とを間に設けられたデータ伝送のためのインタフェイスである。又、端末装置として、ＶＴＲ装置（Ａ）１０３０、ＶＴＲ装置（Ｂ）１０４０、記録装置（Ｃ）１０５０、更にＴＶ装置（Ｄ）が、データ伝送ライン１０７０によりＳＴＢ１０２０と接続されている。

【０００８】次に、同図を参照しながら、ＳＴＢ１０２０の内部構成について更に述べる。

【０００９】尚も、受信手段１０２１は、アンテナ１０１０と接続し、受信したデータの復調を行い、その受信データに施されている伝送用スクランブルを解除し、更に、多重化されている受信データを分離する手段である。暗号化手段１０２２は、ＡＶ機と端末装置との暗号化のためのワークキーＫｗにより、受信手段１０２１から出力されてきたＡＶデータを圧縮状態のまま暗号化する手段である。又、暗号化手段１０２２は、認証手段１０２３から得たサブキーを用いて、ワークキーＫｗを暗号化し、その暗号化したワークキーと、上記暗号化したＡＶデータの双方をデータ入出力手段１０２４を介して、端末装置へ出力するための手段である。尚、ここで、上記の様に暗号化されたワークキーをも端末装置へ送る必要があるのは、端末装置では、転送されてきたＡＶデータを復号化した上で、記録等することを前提としているからである。認証手段１０２３は、ＡＶデータの転送相手をしてきた端末装置との間で、双方の装置が正規の装置であるかどうかをお互いに確かめ合うため、所定の秘密鍵を利用して認証作業を行い、その結果として、認証相手に対応したサブキーを生成する手段である。又、認証手段１０２３は、あらゆる端末装置が有する固有の全ての識別番号（Ｓａ，Ｓｂ，Ｓｃ，Ｓｄ，・・，Ｓｎ，・・・）を、それらの識別番号となりうる値で保有している。データ転送方手段１０２４は、ディジタル・インタフェースとしておもれている１ＥＥＥ１３９４である。データ転送手段１０２４は、リアルタイム性の保証が必要となる映像や音の様なデータの転送に適したアイソクロナス転送と、その必要のない記録用データやコマンド等の転送に適したアシンクロナス転送の２つの転送を行う手段である。

【００１０】次に、ＶＴＲ装置（Ａ）１０３０の内部構成について、更に述べる。

【００１１】同図に示すとおり、データ転送手段１０３１は、データ転送手段１０２４と同様の手段であり、暗号化されたワークキー及び暗号化されたＡＶデータを受け取る手段である。認証手段１０３２は、固有の値Ｓｘをその行いてから、認証作業の結果として、サブ

キーKssを生成して、暗号化手段1033へ出力する手段である。暗号化手段1033は、データ転送手段1031から得た暗号化されたワークキーをサブキーKssにより復号化してワークキーKwを復元し、そのワークキーKwにより、格納されたAVデータを暗号化する手段である。記録・再生手段1034は、暗号化されたAVデータを記録し、又、その記録データを再生する手段である。

【0012】尚、その他の端末装置である、VTR装置(B)1040、記録装置(D)1050、TV受像機(D)1060も、記録・再生手段を除き、上記VTR装置(A)1030の構成と基本的に同じである。但し、S2認証手段が予め有する秘密関数は、上記各装置の観点でいえば、Sb、Sc、Sdである。従って、各装置と、STB1020との認証作業により生成されるサブキーは、上記の符号でいえば、Kssb、Kssc、Kssdである。

【0013】以上の構成において、次に、認証作業の内容を簡単に述べる。

【0014】例えば、VTR装置(A)1030からSTB1020に対して、AVデータの転送要求を行う場合、その実行に先立ち次のような認証作業が必要となる。

【0015】即ち、先ず、VTR装置(A)1030の認証手段1032が、乱数A1、A2を発生させ、これを秘密関数Ssにより暗号化する。ここで、暗号化された乱数をEs(A1,A2)と記載する。認証手段1032は、Es(A1,A2)とその識別番号IDsとデータ処理手段1031をおして、STB1020へ転送する(ステップ1001)。ここで、識別番号は、各端末装置固有の番号で予め与えられている。

【0016】STB1020では、認証手段1023がデータ転送手段1024を介して、Es(A1,A2)と識別番号IDsとを受け、その識別番号を認識して、それに対応する秘密関数Ssを、保有している複数の秘密関数の中から選択する(ステップ1002)。これにより、STB1020が、VTR装置(A)1030との間の通信に使用すべき秘密関数が特定される。

【0017】次に、STB1020の認証手段1023が、秘密関数Ssを用いて、上記受信したEs(A1,A2)を解読して、復元したA1,A2の内、乱数の乱数A2を、暗号化せずにVTR装置(A)1030へ送る(ステップ1003)。

【0018】次に、VTR装置(A)1030の認証手段1032が、STB1020から送られてきたA2と、自らが、上記ステップ1001で発生させた乱数A2とを比較する。双方が一致すれば、STB1020の正規の装置であると判断される(ステップ1004)。

【0019】次に、STB1020側の認証手段1023が、乱数B1,B2を発生させ、これを秘密関数Ssにより暗号化する。そして、Es(B1,B2)をVTR装置(A)1030へ転送する(ステップ1005)。

【0020】VTR装置(A)1030では、認証手段1032の秘密関数Ssを用いて、上記受信したEs(B1,B2)を解読して、復元したB1,B2の内、後者の乱数B2を、暗号化せずにSTB1020へ送る(ステップ1006)。

【0021】次に、認証手段1023が、VTR装置(A)1030から送られてきたB2と、自らが、上記ステップ1005で発生させた乱数B2とを比較する。双方が一致すれば、VTR装置(A)1030が正規の装置であると判断出来る(ステップ1007)。

【0022】以上により、双方が共に正規の装置であることが互いに確認出来き、認証作業が完了し、VTR装置(A)1030へのAVデータの転送が許可される。

【0023】この認証作業の結果、4つの乱数A1,A2,B1,B2が、双方の装置の認証手段1023,1032には存在している。そこで、次に、双方の認証手段1023,1032がそれぞれ、乱数A1,B1を用いて上記サブキーKssを生成する。尚、サブキーの生成に際し、乱数A2,B2を使用しないのは、これらは、暗号化せずに転送されたという経緯があるため、その様な経緯の無い乱数A1,B1を使用する方が、キーの安全性から見て、より優れているからである。

【0024】暗号化手段1032では、この様にして生成されたサブキーKssを用いて、ワークキーKwが暗号化され、又、AVデータはワークキーKwで暗号化される。そして、上記暗号化されたワークキーKss(Kw)と、暗号化されたAVデータKw(AV)の双方がデータ入出力手段1024を介して、VTR装置(A)1030へ出力される。

【0025】VTR装置(A)1030では、復号化手段1033が、認証手段1032から得たサブキーKssを用いて暗号化ワークキーKss(Kw)の復号をし、復号された ワークキーKwを用いて暗号化AVデータKw(AV)の復号を行うものである。

【0026】

【発明が解決しようとする課題】しかしながら、上記の様な認証方法では、不正者が、正規な装置の秘密関数Ssと識別番号IDsとをそっくりそのまま模倣して、上記と同じ認証方法を行える不正な装置を製造・販売し、その不正装置が使用された場合、上記認証方法では、その装置が不正な装置であることを見破ることが出来ず、AVデータの転送を阻止することが出来なかった。

【0027】一般に、暗号キャッシュカード等の第3者による不正使用では、そのキャッシュカードの持ち主に対して、直接的な損害に発生する。そのため、不正使用を直ちに阻止することが可能でもあり、これに対して、放送データの受信機や装置として、上記の様な不正

装置が存在していても、関係者に対する被害が表面化し難いという特殊性がある。例えば、コピー禁止のデータを不正にコピーしても、著作権料等が未払いであるというような具体的な被害が表面化することは稀であり、更に表面化したとしても、それまでにはかなりの時間が経過しており、被害は甚大になることも予想される。

【0028】この様に、従来の認証方法では、被害が明るみに出てからしか対応が出来ないため、認証方法として不完全であるという課題を有していた。

【0029】本発明は、この様な従来の方法の課題を考慮し、不正な装置の検出を従来に比べてより確実に行える管理基準作成方法、管理基準作成システム、及び媒体を提供することを目的とする。

【0030】

【課題を解決するための手段】請求項1記載の本発明は、それぞれ固有の識別子を有する各データ要求端末装置からデータ転送装置に対しデータ要求が有った際、それらのデータ要求に関して、所定の認証基準に基づいた認証を行い、前記認証の結果に応じて、前記データ転送装置から、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定し、常に、又は前記認証の結果に応じて、前記データ転送装置から管理装置に対して、そのデータ要求端末装置の前記識別子を含むデータ要求履歴情報を送り、前記管理装置は、前記送られてくるデータ要求履歴情報を利用して、所定の判定基準により、そのデータ要求履歴情報に含まれたデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新する管理基準作成方法である。

【0031】請求項8記載の本発明は、それぞれ固有の識別子を有する各データ要求端末装置に接続されたデータ転送装置を単数又は複数管理する管理装置が、送られてくる、新規に接続される予定の又は新規に接続された前記データ要求端末装置の識別子を含む新規登録情報を利用して、所定の判定基準により、前記新規登録情報に対応するデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新する管理基準作成方法である。

【0032】請求項11記載の本発明は、それぞれ固有の識別子を有する複数のデータ要求端末装置と、それらデータ要求端末装置からデータ要求が有った際、それらのデータ要求に関して、所定の認証基準に基づいた認証を行い、(1)その認証の結果に応じて、前記データ要求を行ったデータ要求端末装置に対して、その要求されたデータを転送するかどうかを決定し、又、(2)常に、又はその認証の結果に応じて、そのデータ要求端末装置の前記識別子を含むデータ要求履歴情報を出力するデータ転送装置と、前記出力された前記データ要求履歴情報を得て、所定の判定基準により、そのデータ要求履歴情報に含まれたデータ要求端末装置が正規なものであるか否かを判定し、その判定結果に基づいて管理基準を作成、又は更新する管理装置とを備えた管理基準作成システムである。

【0033】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【0034】(第1の実施の形態)図1は、本発明の一実施の形態における管理基準作成システムの構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の管理基準作成システムの構成について述べる。

尚、本実施の形態では、図12で説明したものと、基本的に同じ構成のものには、同じ番号を付し、その詳細な説明は省略した。

【0035】図1に示す様に、管理装置110は、各所に存在する第1のSTB120、・・・、第nのSTB130及び各端末装置を管理する装置である。又管理装置110は、各STBが認証作業において利用するための不正装置リストを作成し、更新する手段である。通信回線140は、管理装置110と各STB120、130との間のデータ伝送に利用する手段である。本実施の形態では、第1のSTB120は北海道のAさん宅に、又、第nのSTBは沖縄のNさん宅に設けられているとする。

【0036】又、各STB120、130には、データ伝送ライン1076上で、端末装置がそれぞれ接続されている。即ち、図1に示す通り、第1のSTB120には、VTR装置1030、VTR装置1040、記録装置1050)、及びTV装置1060が接続されており、又、第nのSTB130には、VTR装置150、記録装置160、及びTV装置170が接続されている。ここで、VTR装置150が不正装置であるとする。この不正装置は、後述するライセンスキー及びEUI64として、正規のVTR装置1030のものをそっくりそのまま模倣することにより不正に製造された装置であるものとする。

【0037】尚、これら、各端末装置は、図12にて説明した通り、データ転送手段1031としてIEEE1394を備えている。又、本実施の形態では、これら端末装置は、それぞれIEEE1394におけるEUI64を、各装置固有の番号、即ち、識別番号として予め備えている。ここで、EUI64は、64ビットの識別コードである。又、これら端末装置は、その識別番号に対応したライセンスキーを備えている。このライセンスキーは、正規の端末装置にのみ与えられる非公開の秘密鍵であるが、EUI64の識別番号は、データ転送時に誰でも知り得るいわゆるID番号である。以下、EUI64の識別番号を単に、EUI64、又はID番号と呼ぶ。尚、各STB120、130についても、固有のEUI64が設けられている。これら識別番号は各装置に対して、一対一に対応しており、重複することはない。

9

【００３８】次に、図２を参照しながら、ＳＴＢ１２０の内部構成について、更に詳細に述べる。

【００３９】図２に示す通り、ＳＴＢ１２０は、図１３に示すように手段１０２３の構成に加えて、データ要求履歴情報記憶手段２１０、モデム２１３、ＣＲＬ記録手段２１４、及びＣＲＬ格納手段２１５を備える。

【００４０】認証手段２１１は、ライセンスキーと同じキーであるサービスキーを作ることが出来るサービスキー生成関数を備えている点と、認証において、後述するＮＧ装置のリストを参照する点で、図１２で述べた認証手段１０２３と相違する。このサービスキー生成関数は、端末装置から得られたＥＵＩ６４（ＩＤ番号）から、サービスキーを生成する関数である。そのため、認証手段２１１は、端末装置のＥＵＩ６４を予め記憶しておく必要がない。

【００４１】データ要求履歴情報記憶手段２１２は、端末装置から所定の放送番組のデータ転送要求があった場合、後述する認証作業を経て、要求データの転送が完了したものについて、そのデータ要求に関する履歴情報を生成し、その記憶に関する手段である。このデータ要求履歴情報は、データ転送完了した端末装置のＥＵＩ６４と、その端末装置からのデータ要求の有った時刻を特定する時刻情報と、その端末装置の所在を特定する所在情報から構成されている。尚、データ要求履歴情報記憶手段２１２は、これらＥＵＩ情報～所在情報を認証手段２１１から得る。又、データ要求履歴情報記憶手段２１２は、１ヶ月間の各端末装置からのこのような履歴情報を記憶しておき、１ヶ月前に、モデム２１３を介して、管理装置１１０へ送る手段である。

【００４２】又、ＣＲＬ記録手段２１４は、管理装置１１０から送られてくる不正装置を記載したリストデータをモデム２１３から得て、ＣＲＬ格納手段２１５に記録・更新する手段である。ＣＲＬ格納手段２１５は、不正装置のリストデータを格納するためのメモリ手段である。尚、本明細書では、不正装置のリストを、単にＣＲＬ（Certification Revocation List）と呼ぶ。又、請求項１記載の本発明の管理装置は、ＣＲＬに対応する。

【００４３】次に、図３を参照しながら、管理装置１１０の内部構成について、更に詳細に述べる。

【００４４】図３に示す通り、履歴情報記憶手段１１３は、モデム１１１を介して、各ＳＴＢ１２０，１３０から１ヶ月前に同時期に送信されてくる各データ要求履歴情報を、送信元のＳＴＢのＥＵＩ６４と対応させて、一時的に記憶する手段である。不正装置決定手段１１２は、上記履歴情報記憶手段１１３に記憶されている各ＳＴＢからの１ヶ月分の全てのデータ要求履歴情報の中で、同一のＥＵＩ６４が複数存在する場合、それら複数のＥＵＩ６４に対応する時刻情報と所在情報をそれぞれ比較して、不正の可能性があるＥＵＩ６４を有するデータ要求端末装置を決定する手段である。ＣＲＬ作成手段１１４は、不正装置決定手段１１２から１ヶ月毎に出力される上記決定結果を得て、不正装置のリストを作成し、出力する手段である。尚ＣＲＬ記録手段１１５は、ＣＲＬ作成手段１１４からのリストデータを得て、既に記録されているリストに対し、新たな不正装置の追加や、データの修正等を行い、全ての地域の端末装置に関する全ＣＲＬを管理する手段である。最新ＣＲＬ作成手段１１６は、各ＳＴＢに対応した個別のＣＲＬを作成し、モデム１１１を介して、対応するＳＴＢに送信する手段である。最新のＣＲＬは、ＳＴＢ等にまとめられた不正装置のリストであり、不正装置が検出されていないＳＴＢについては作成されない。

【００４５】以上の構成において、次に、主に図４～図６（ａ）を参照しながら、本実施の形態の動作を述べ、同時に本発明の管理装置作成方法に係る一実施の形態についても説明する。尚、図４は、１９９７年１月１日から、同月３１日までの、ＳＴＢ１２０におけるデータ要求履歴情報記憶手段２１２の記憶内容を説明する図であり、図５は、１９９７年１月１日から、同月３１日までの、管理装置における履歴情報記憶手段１１３の記憶内容を説明する図である。

【００４６】ここでは、１９９７年１月３１日の時点では、ＳＴＢ１２０のＣＲＬ格納手段２１５のＣＲＬ（不正装置のリスト）には、不正装置はまだ記載されていない、即ち、空の状態であるとする。又、ＳＴＢ１３０のＣＲＬ格納手段のＣＲＬについても、空の状態である。

【００４７】又、ここでの説明は、先ず、（１）ＳＴＢにおける、ＣＲＬを利用した認証動作について述べ、次に、（２）管理装置におけるＣＲＬの作成及び、ＳＴＢへのＣＲＬの送信について述べ、最後に、（３）ＳＴＢにおける、ＣＲＬの更新動作を述べる。

（１）ＳＴＢにおける、ＣＲＬを利用した認証動作：ここでは、ＳＴＢ１２０が、受信手段１０２１により受信した映像番組のＡＶデータについて、例えば、正規の装置であるＶＴＲ装置１０３０からの転送要求を受けた場合、次のような認証動作を行う。尚、この転送要求は、図４、図５中に記載されている履歴情報の内、平成１０年１月１０日午前１２時１０分にあった要求に対応している。

【００４８】ステップ１：先ず、ＳＴＢ１２０の認証手段２１１は、転送要求をしてきたＶＴＲ装置１０３０のＥＵＩ６４（ここでは、１１０３０番とする）をデータ転送手段１０２４から得る。

【００４９】ステップ２：そして、認証手段２１１は、ＣＲＬ格納手段２１５のＣＲＬを参照して、そのＥＵＩ６４と同じ番号が不正装置の番号としてＣＲＬの中に登録されていないかどうかをチェックする。この時点では、上記の通り、ＣＲＬは空の状態であるため、そのＥＵＩ６４は未登録であるとの判定結果が出て、本格的な認証作業に入る（ステップ３）。尚、このチェック段階

11

て、ＣＲＬに登録されているとの判定が得ると、その後の認証作業は行わず、要求のあったデータの転送は行わない。

【００５０】ステップ３：認証手段２１１は、ステップ１で得たＶＴＲ装置１０３０のＥＵＩ６４を用いて、サービスキー生成関数からサービスキーを生成する。この様にして生成されたサービスキーは、ＶＴＲ装置１０３０が有するライセンスキーと同一の値である。尚、ライセンスキー及びサービスキーは、図１９で述べた処理部９ａに対応する。

【００５１】認証手段２１１は、この様にして生成したサービスキーを用いて、一方、ＶＴＲ装置１０３０は、予め与えているライセンスキーを用いて、双方の間で、図１８で既に説明したものと同様の認証作業を行う。即ち、双方の装置が、それぞれ乱数ＡＬ，Ｂ１を用いて、同一のサブキーＫｓａを生成する。

【００５２】ステップ４：暗号化手段２０２２は、上記サブキーＫｓａを用いて、ワークキーＫｗを暗号化し、且つ、データキー長ｗを用いて、入Ｖデータを部分化し、それら双方の暗号化データ（Ｋｓａ（Ｋｗ），Ｋｗ（ＡＶ））をＶＴＲ装置１０３０へ転送する。

【００５３】尚、この認証の過程で、例えば、端末装置からもらってきたＥＵＩ６４が、その端末装置が有するライセンスキーとの定められた対応関係を有していない、全くでたらめな番号であるとすると、サービスキー生成関数により生成された鍵は、そのライセンスキーとは一致しなくなる。というのは、サービスキー生成関数は、上記予め定められた対応関係に基づいて、ＥＵＩ６４からサービスキーを生成するように構成されているからである。従って、この場合、双方の装置の有するキーが同一であることを前提とした上記認証は成立しなくなり、この場合、要求されたデータの転送は行われない。

【００５４】ステップ５：データ要求履歴情報記録手段２１２は、ステップ４にてデータ転送が完了したものに関して、認証手段２１１から、その相手先であるＶＴＲ装置１０３０のＥＵＩ６４として、１１０３０番と、要求の有った時刻情報として、平成１０年１月１０日の時１２時１０分のそれぞれの情報を得て、データ要求履歴情報として記録する（図４参照）。ここで、図４の記載について説明する。即ち、同図において、端末装置のＥＵＩ６４の欄４０１に記載された番号としての、３１０６０番，１１０４０番，１１０３０番，及び２１０５０番は、前から順に、ＴＶ装置１０６０、ＶＴＲ装置１０４０，ＶＴＲ装置１０３０，そして記録装置１０５０のＥＵＩ６４を示している。

【００５５】ステップ６：各端末装置１０３０～１０６０からのデータ転送要求が有る毎に、上記ステップ１～５を上記と同様に実行する。そして、データ要求履歴情報記録手段２１２は、１ヶ月間に記録蓄積された各履歴データ（図４参照）に、ＳＴＢ１３０のＥＵＩ６４（ここでは、９００１番とする）及びその所在情報としての電話番号を加えたものをデータ変化規則情報として（モデム２１３から電話回線１４０を介して、１ヶ月毎に管理装置１１０へ転送する。

（２）管理装置におけるＣＲＬの作成及び、ＳＴＢへのＣＲＬの配信動作：ここでは、管理装置１１０の動作を述べる。

【００５６】ステップ１０１：管理装置１１０の履歴情報記憶手段１１２には、各地のＳＴＢ１２０～１３０から１ヶ月毎に上述したデータ要求履歴情報がモデム１１１を介して転送されてくる。履歴情報記憶手段１１２は、これらの情報を時間順として保存する。

【００５７】ステップ１０２：不正装置決定手段１１３は、履歴情報記憶手段１１２に保存された履歴情報を基に、その時刻情報により、データ内容を時間順に並べ変える（図５参照）。図５は、並べ変えられた履歴情報の内容を説明するための図である。

【００５８】そして、端末装置のＥＵＩ６４の欄５０１（図５参照）に示す端末装置のＥＵＩ６４が同一のものがあれば、それらに対応する時刻情報及びその所在情報をそれぞれ比較して、不正の可能性があるＥＵＩ６４に対応する端末装置を決定する。

【００５９】即ち、図５に示す場合、符号５１１、５１２、５１３の付された各行に記載された端末装置のＥＵＩ６４が、全て１１０３０番である。ここで、これらが完全チェックされる、符号５１１と５１２の付された行の時刻情報同士を比較するとそれぞれ異なる時刻における転送要求の発生であり、双方の装置に矛盾はないと判断できる。しかし、符号５１２と５１３を付した行に記載された二つの情報は、同一のＥＵＩ６４を有する装置は存在しないという前提と矛盾する状況が発生していることを示している。尚、図５のＳＴＢのＥＵＩ６４の欄５０４に記載された番号９００１０は、ＳＴＢ１３０のＥＵＩ６４である。

【００６０】即ち、不正装置決定手段１１３は、これら双方の時刻情報の欄５０２及び所在情報の欄５０３のデータを比較した際、一方は神奈川、他方は北海道という地理的に遠く離れた場所から、１０分違いで、同一のＥＵＩ６４を有する装置により転送要求が有ったという事実から見て、同一のＥＵＩ６４を有する装置が、北海道のＡさん宅と、沖縄のＮさん宅に存在すると判断する。そして、不正装置決定手段１１３は、これら双方の装置の双方ともが不正な装置であると考え、その判定結果をＣＲＬ作成手段１１４へ送る。尚、沖縄のＮさん宅に設置されているＶＴＲ装置１５０が完全に不正な装置であるとしたが、この段階では、何れが積極に不正な装置であるのかというところまでは、分からないので、とりあえず双方を不正と見なすものである。尚、何れが不正であるかの判定については、後述する。又、符号５２１、５２２を付した行に記載された履歴データに対した対

異なるときは、同一のＥＵＩ６４を有する装置は存在しないという前提と矛盾する状況は見あたらない。

【００６１】ステップ１０３：ＣＲＬ作成手段１１４は、不正装置決定手段１１３から得られた判定結果から、図６（ａ）に示す様なＣＲＬを作成して、全ＣＲＬ記録手段１１５へ送る。この様な、ＣＲＬの作成動作は、毎月行われ、その度に、全ＣＲＬ記録手段１１５に記録する。従って、全ＣＲＬ記録手段１１５は、ＣＲＬ作成手段１１４から送られてくるリストにより、既に記録しているＣＲＬに追加、訂正などを加えて、その都度、更新するものである。

【００６２】ステップ１０４：個別ＣＲＬ作成手段１１６は、ＣＲＬ作成手段１１４で作成された全ＣＲＬにおけるＳＴＢのＥＵＩ６４の値６０１を抜き出して、そのＣＲＬの内容をＳＴＢ毎に分離する。図６（ｂ），（ｃ）は、それぞれ、ＳＴＢ１３０，ＳＴＢ１２０に配信するために作成された個別ＣＲＬである。個別ＣＲＬ作成手段１１６は、これらの個別リストを対応するＳＴＢへ、モデム１１８を介して配信する。

（３）ＳＴＢにおける、ＣＲＬの更新動作：管理装置１１０から配信されてきた個別ＣＲＬ（図６（ｃ）参照）を得た、ＳＴＢ１２０は、次の様な動作を行う。

【００６３】ステップ２０１：同様、ＣＲＬ記録手段２１４は、モデム２１３から上記個別ＣＲＬを得て、それまで空の状態であったＣＲＬ格納手段２１６に記録する。これによりＣＲＬ格納手段２１６には、ＳＴＢ１２０に接続されているＶＴＲ装置１０３０（ＥＵＩ６４が１０３０番）が不正装置として格納される。従って、今後、このＶＴＲ装置１０３０からのデータ転送要求があっても、上記ステップ２の段階で不正装置であることが判明するので、データ転送は行われない。これにより、不正装置による被害の拡大が防止出来る。尚、ＳＴＢ１３０においても、全く同様の動作が行われる。この場合は、ＳＴＢ１３０のＣＲＬ格納手段には、ＶＴＲ装置１５０（ＥＵＩ６４が１１０２０番）が不正装置として登録される。

【００６４】（第２の実施の形態）図７，８は、本発明の一実施の形態における管理基準作成システムを構成するＳＴＢ及び管理装置の構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の管理基準作成システムの構成について述べる。尚、本実施の形態では、第１の実施の形態で説明したものと、基本的に同じ構成のものには、同じ符号を付し、その詳細な説明は省略した。又、本実施の形態のシステム全体の構成は、基本的に図１で述べたものと同じである。

【００６５】本実施の形態と上記実施の形態の主な相違点は、端末装置についての不正・非不正判定情報の作成のプロセスである。従って、ここでは、この相違点を中心に説明する。尚、請求項５に記載の本発明の管理基準は、不正・正規判定情報に対応する。

【００６６】図７に示すＳＴＢ１２０の構成において、図２で示した構成と相違する主な点は、新規接続装置検出手段７１１と、不正・正規情報抽出手段７１２と、不正・正規情報記録手段７１３が、図２のデータ蓄積管理手段２１２、ＣＲＬ格納手段２１５と、ＣＲＬ記録手段２１４の代わりに設けられていることである。更に、認証手段７１４は、第１の実施の形態で述べたものとは異なり、新規接続からのデータ転送要求に関する認証情報を出力する構成にはなっていない。尚、その他の構成は、同じである。

【００６７】新規接続装置検出手段７１１は、ＳＴＢ１２０のデータ伝送ライン１０７０に新たに接続された装置が有った場合、それを検出し、そのＥＵＩ６４を取得する手段である。取得したＥＵＩ６４は、ＳＴＢ１２０のＥＵＩ６４と共に、モデム２１３から、管理装置１１０へ送られる。この動作は、新に接続された装置の管理装置への不使用登録のための作業であり、同時に、その新規接続装置が不正でないかどうかも確認するための作業でもある。尚、この動作は、新規登録の際に行うものであるから、上記第１の実施の形態で述べたデータ転送要求の度に行うものとは異なり、初回のみの動作である。

【００６８】不正・正規情報記録手段７１３は、管理装置１１０から送られてくる情報を不正・正規情報抽出手段７１２に振り分ける手段である。

【００６９】次に、図８を参照しながら、管理装置１１０の構成を述べる。

【００７０】同図に示すように、照会手段８１１は、ＳＴＢ１２０～１３０から送られてくる、新規接続情報としての、新設された端末装置のＥＵＩ６４とその送信元のＳＴＢのＥＵＩ６４とを得て、それが不正であるかどうかを判定する手段である。新規登録装置一覧情報記憶手段８１２は、照会手段８１１から得た新規登録装置のＥＵＩ６４を記憶する手段である。

【００７１】又、不正・正規判定情報作成手段８１３は、照会手段８１１による上記チェック結果から新規登録のあった装置について、不正であるか、あるいは正規であるかの判定情報を作成し、その何れかの情報をモデム１１１を介して、対応するＳＴＢに送信する手段である。尚、不正・正規判定情報作成手段８１３は、通信先となった場合、そのＥＵＩ６４を有する方の装置を不正装置と見なし、ＳＴＢ毎に対応する不正情報のリスト（図６（ｂ），（ｃ）参照）を作成し、配信するものである。

【００７２】以上の構成において、次に、主に図９（ａ）～図１０（ｂ）を参照しながら、本実施の形態の動作を述べ、同時に本発明の管理基準作成方法に係る一実施の形態についても説明する。尚、説明の都合上、本実施の形態では、図１におけるＶＴＲ装置１０４０，記録装置１０５０，及びＴＶ装置１０６０は、既にＳＴＢ１

２０に接続であり、又、ＶＴＲ装置１５０、記録装置１５０、及びＴＶ装置１７０は、共にＳＴＢ１３０に接続であり、これらの端末装置については、以下に説明する機能を備えているものとする。又、ＶＴＲ装置１０３０は、ＳＴＢ１３０に対して、新たに接続される装置であるとする。尚、ＶＴＲ装置１５０は、上記実施の形態でも説明した通り、不正装置であるとする。ここでの説明は、先ず、（１）ＳＴＢにおける、新規に接続される装置の検出動作について述べ、次に、（２）管理装置における、新規登録及び不正・正規判定情報の作成等について、最後に、（３）ＳＴＢにおける、不正・正規判定情報の更新及び、不正・正規判定情報を利用した認証動作について述べる。尚、これらの説明は、第１の実施の形態との相違点を中心に行う。

（１）ＳＴＢにおける動作：上述の通り、ＳＴＢ１３０に対し、ＶＴＲ装置１０３０が、新たに接続されたとする（図７参照）。

【００７５】ステップ２０１：図７に示す新規接続装置検出手段７１１は、データ伝送ケーブル１０７に接続されている全ての端末装置のＥＵＩ６４を、定期的に読み出し、内部するメモリ（図示省略）に記録する。そして、既に記録されている前回検出のＥＵＩ６４の記録データと比較する。

【００７６】ＶＴＲ装置１０３０が新たに接続された状態では、上記ＥＵＩ６４の定期的な読み出し、及び上記比較動作により、ＥＵＩ６４が１１０３０番の装置が、新規に接続されたことが検出される。

【００７７】ステップ２０２：更に、新規接続装置検出手段７１１は、上記検出した新規装置の対象となる装置のＥＵＩ６４（１１０３０番）と、通信元のＳＴＢ１２０のＥＵＩ６４（９０１２０番）とを新規登録情報として、モデム２１４を介して管理装置１１０へ送信する。

（２）管理装置における動作：図９（ａ）は、ＶＴＲ装置１０３０が登録される前の、新規登録前一覧情報記憶手段８１２の記憶内容を説明するための図であり、図９（ｂ）は、ＶＴＲ装置１０３０が登録された後の図である。これらの図面を参照しながら、説明する。

【００７８】ステップ３０１：図８に示す照合手段８１１は、ＳＢＴ１２０から送信されてきた新規登録情報を元に、新規登録装置一覧情報記憶手段８１２の記憶内容（図９（ａ）参照）を調べ、その登録が、重複登録というような状態を生じさせないかどうかをチェックする。新規登録情報に含まれているＥＵＩ６４は１１０３０番であり、これは、図９（ａ）に示す様に、既に登録済のもの（図９（ａ）中、符号９０１を付した）と重複する。従って、照合手段８１１は、登録した双方のＥＵＩ６４について、不正であると判定し、出力する。

【００７７】ステップ２０２：新規登録装置一覧情報記憶手段８１２は、照合手段８１１から送られてくる新規登録情報の内容を登録（図中、符号９０２を付した）す

る。更に、上記判定結果から、重複した双方のＥＵＩ６４について、備考欄９０３に、不正である旨の情報を記録する。尚、それ以外に不正であるものの判定については、後述する。

【００７９】ステップ３０３：不正・正規判定情報作成手段８１３は、照合手段８１１から送られてくる判定結果から、図１０（ａ）、（ｂ）に示すような、不正・正規判定情報のリストを作成する。これらリストは、ＳＴＢ毎にまとめられている。図１０（ａ）、（ｂ）では、上述の通り、何れＳＴＢの欄１０１に、不正を示す情報が記録されている。但し、ステップ３０１における、照合手段８１１による新規登録情報の判定の結果、それが正規であると判定された場合、判定結果の欄１０１には、当うまでもなく正規を示す情報が記録される。

【００７９】ステップ３０４：不正・正規判定情報作成手段８１３は、上記のようにして作成した判定結果の例リストをモデム２１１を介して、ＳＴＢ１２０とＳＴＢ１３０とに送信する。この送信は、上述した新規登録情報がＳＴＢから送られてくる度に実行される。

【００８０】（２）ＳＴＲにおける動作：図１１（ａ）は、不正・正規情報格納手段７１２に既に格納されている内容を示す図であり、図１０（ａ）に示す判定結果の例リストが送信されるＳＴＢの状況を示している。又、図１１（ｂ）は、図１０（ａ）に示す判定結果の例リストの内容が更新された後の状況を示している。

【００８１】図７に示す不正・正規情報記録手段７１０は、管理装置１１０から送信されてきた判定結果の例リストをモデム２１３から介して、これを図１１（ａ）に示す記録内容に対して追加する。図１１（ｂ）の上から第４行目（図中、符号１１３を付した）に、上記例リストの内容が追加されている。同図の判定結果の欄１１１には、当該端末装置のＥＵＩ６４の欄１１３に示した装置が不正であるか正規であるかを示している。

【００８２】一方、ＳＴＢ１３０においても、上記と全く同様の動作が行われる。

【００８３】次に、ＶＴＲ装置１０３０から、ＳＴＢ１２０に対して、ＡＶデータの転送要求が有った場合について述べる。

【００８４】この場合は、第１の実施の形態で述べたステップ１～ステップ４で述べた認証動作において、上記ステップ２の内容のみが異なるので、その相違点のみ述べる。

【００８５】即ち、上記ステップ１と同様の動作の後、認証手段７１４は、不正・正規情報格納手段７１２を参照して、転送要求をだした端末装置のＥＵＩ６４が正規であるか不正であるかをチェックする。図１１（ｂ）に示す通り、符号１１３を付した行に記録された情報によると、上記転送要求をしてきたＥＵＩ６４が１１０３０番の装置は、不正であることが示されている。従って、認証手段７１４は、その後の認証作業は行わず、要

17

求のあったデータの転送しかのない。

【００８６】また、チェックの結果、正規である場合、上記ステップ３～４で述べたのと同様の動作を行う。

【００８７】又、転送要求の有った装置のＥＵＩ６４が、不正・正規情報格納テーブル７１２に未登録の場合、認証手段７１４は、新規機器認証検出手段７１１に対して、その要求元の装置の識別情報を管理装置１１０へ送るように指示する。、これにより、不正装置による被害の拡大が防止出来る。

【００８８】ところで、上述した通り、ある装置が不正であると判定された場合、その誤れが本当に不正であるのかの判定について述べる。

【００８９】この場合、ＳＴＢにより不正であると見なされて、要求したデータを送ってもらえなかった使用者は、その不正判定を受けた装置の誤りをはらすため、管理装置１１０を所有する管理センターに、調査を依頼することが可能である。調査依頼を受けた管理センターは、その装置の状態を調査して、不正な方法により製造又は改造されたものでないかどうかを厳密にチェックする。そして、正規であると判明すれば、管理装置に記録されているデータを修正し、その修正結果を保有するＳＴＢへ転送する。これにより、正規であると判明した装置に対しては、転送要求に応じることとなる。

【００９０】又、以上述べた実施の形態の何れかひとつに記載の各ステップ（又は手段）の全部又は一部のステップ（手段）をコンピュータに実行させるためのプログラムを記録した磁気記録媒体や半導体メモリなどを作成し、これを利用して上記と同様の動作を実行させることも出来る。この場合も上記と同様の効果を発揮する。

【００９１】尚、上記実施の形態では、端末装置から有った全てのデータ転送要求を対象として、データ要求記録情報記憶手段７１３に記録する場合について述べた。が、これに限らず例えば、重要なデータの転送要求のみを対象として、記録する構成でも良い。ここで、重要なデータとしては、例えば、記録したら課金するといったペーパレック（ＰＲＯＣ）やペーパービュー（ＰＰＶ）の様なデータである。従って、例えば、チャンネル毎にお金を支払うものや、無料のチャンネルの番組データなどは、対象外としても良い。

【００９２】又、上記第２の実施の形態では、端末装置が新規登録されたことを自動的に検出する場合について述べたが、これに限らず例えば、新規に購入した装置に登録はがきを添付しておき、使用者が、そのはがきを管理装置を所有する管理センターに送る様式としても良い。

【００９３】又、上記実施の形態では、ＣＲＬや不正、正規情報のＳＴＢへの送信を電話回線を用いて行う場合について述べたが、これに限らず例えば、放送にとって送っても良い。

【００９４】又、上記第２の実施の形態では、ＳＴＢ側

18

から送られてきた新規登録情報と、既に送られてきた新規登録情報の最新データとを比較して、重複が無いかどうかをチェックする場合について述べたが、これに限らず例えば、装置を製造した会社から送られてくる生産情報に記載された、工場内の正規装置のＥＵＩ６４の一覧データを保持したメモリを備え、上記目的の際、そのメモリの内容との比較を行う構成でも良い。新規登録情報に含まれたＥＵＩ６４が全くでたらめである場合でも、上記メモリの内容と比較することにより、少なくとも正規装置のＥＵＩ６４とも一致しないような番号であれば、たとえ新規登録装置一覧情報記憶手段７１３に記録されておらず、登録しない状況であったとしても、不正であると判定出来、不正防止の効果が向上する。

【００９５】又、上記実施の形態では、主なる認証動作を行う場合について述べたが、これに限らず例えば、登録内容として、ＣＲＬを登録するのみ、あるいは、不正・正規情報を登録するのみでもかまわない。

【００９６】又、上記実施の形態のある手段の処理動作は、コンピュータを用いてプログラムの後者により、ソフトウェア的に実現してもよいし、あるいは、上記処理動作をコンピュータを使用せずに専用の回路構成により、ハード的に実現してもよい。

【００９７】又、本発明のデータ転送装置は、上記実施の形態では、ＳＴＢであり、そのＳＴＢは、最初に接続されたデータ要求端末装置のＳＴＢとの相互を参照した際、そのデータ要求装置の製造登録情報を管理装置に送信する場合について説明したが、これに限らず例えば、新規接続装置検出手段７１１は、ＶＴＲ装置１０３０から新たに認証を要求された際に、そのＶＴＲ装置１０３０のＥＵＩ６４を得て、既に前項記憶されている不正装置のＥＵＩ６４と比較して、同一のものがなければ、そのＶＴＲ装置１０３０が、新規に接続されたものとして検出する構成でもよい。

【００９８】又、上記実施の形態では、認証の結果、正規な装置であることが確認できた場合に、データを送信装置（ＳＴＢ）から各端末装置に対して、そのデータ要求端末装置の識別子（ＥＵＩ６４）を含むデータを課金情報を送るという例を説明したが、これに限らず例えば、認証の結果に関わらず、管理装置に対して、そのデータ要求端末情報を送る構成でもよい。この場合、装置の最終で、不正な装置であると判明した場合には、その後も課金情報とともに送ればよい。

【００９９】又、上記実施の形態では、ＳＴＢが認証動作の中で、本発明の管理装置（ＣＲＬ又は、不正・正規判定情報）を利用する場合について述べたが、これに限らず例えば、ＳＴＢとしては、その認証動作において、上記ＣＲＬや不正・正規判定情報を使用しない構成でも良い。

【０１００】

19

【発明の効果】以上述べたところから明らかなように本発明は、不正な装置の体外への持ち出しに対してより確実に対処できるという効果を有する。

【図面の簡単な説明】

【図１】本発明の一実施の形態における管理装置作成システムの構成を示す構成図

【図２】同実施の形態におけるＳＴＢの内部構成を示す構成図

【図３】同実施の形態による管理装置の内部構成を示す構成図

【図４】同実施の形態におけるＳＴＢのデータ変換機構終端設定手段の記憶内容を説明する図

【図５】同実施の形態における管理装置の機器情報記憶手段の記憶内容を説明する図

【図６】（ａ）：同実施の形態におけるＣＲＬ作成手段により作成された１ＣＲＬを説明する図

（ｂ）～（ｃ）：同実施の形態における個別ＣＲＬ作成手段により作成された個別ＣＲＬを説明する図

【図７】別の実施の形態におけるＳＴＢの内部構成を示す構成図

【図８】同実施の形態における管理装置の内部構成を示す構成図

【図９】（ａ）：同実施の形態においてＶＴＲ装置が登録された時の、管理情報記憶手段の記憶内容を説明する為の図

20

（ｂ）：同実施の形態においてＶＴＲ装置が登録された後の、管理情報記憶手段の記憶内容を説明する為の図

【図１０】（ａ）～（ｂ）：不正・正規判定情報作成手段による作成された、不正・正規判定情報の個別リストを説明する図

【図１１】（ａ）：図１０（ａ）に示す個別リストが送信された時の、不正・正規情報検索手段における検索内容を示す図

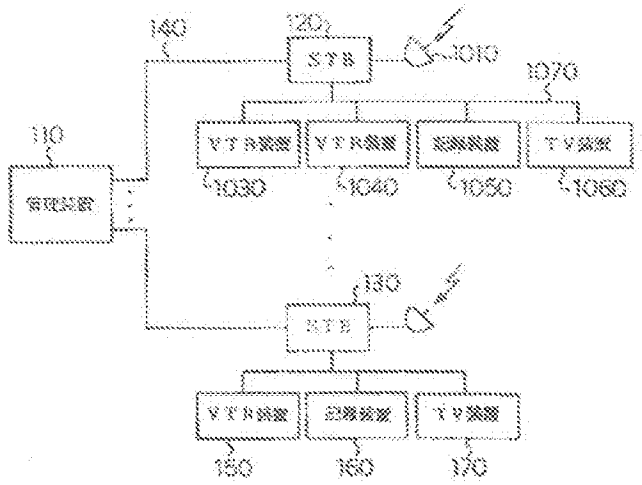
（ｂ）：図１０（ｂ）に示す個別リストが送信された後の、不正・正規情報検索手段における検索内容を示す図

【図１２】従来の専用受信機と端末装置との接続状態及び構成を示すブロック図

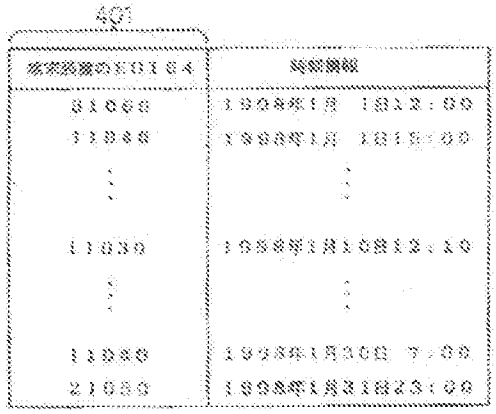
【符号の説明】

１１０	管理装置
１２０	第１ＳＴＢ
１３０	第ｎＳＴＢ
１４０、１０３０、１０４０	ＶＴＲ装置
１５０、１０５０	記録装置
１７０、１０６０	ＴＶ装置
１０１０	アンテナ

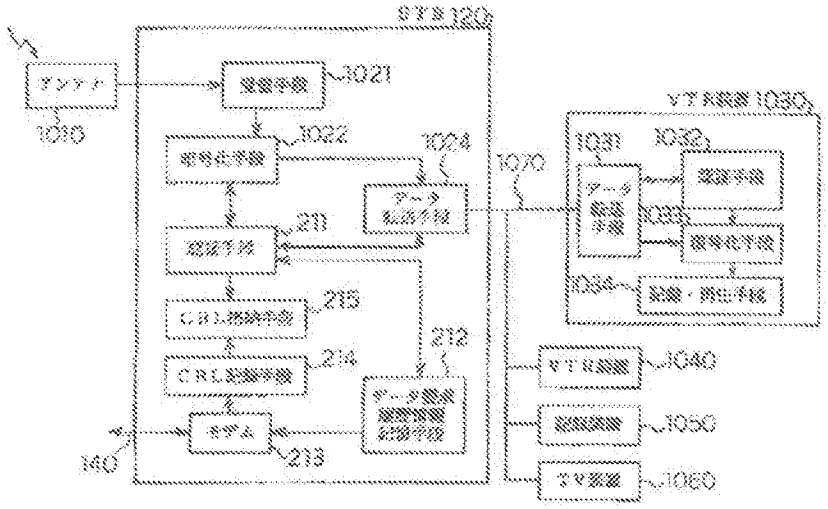
【図１】



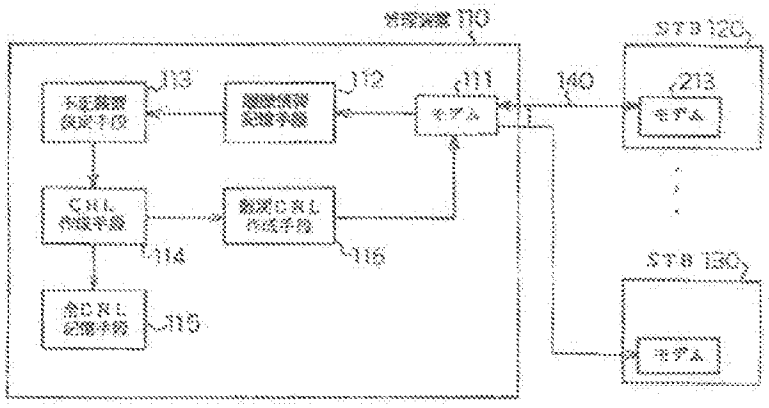
【図４】



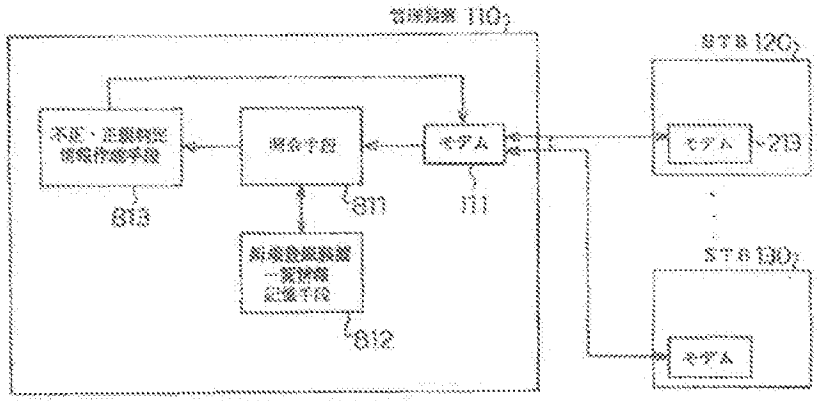
【図２】


STB 120
アンテナ
1010
受信手段
1021
1022
1024
1070
211
215
214
212
213
140
VTR装置 1030
1031
1032
1034
VTR装置
1040
1050
TV装置
1060

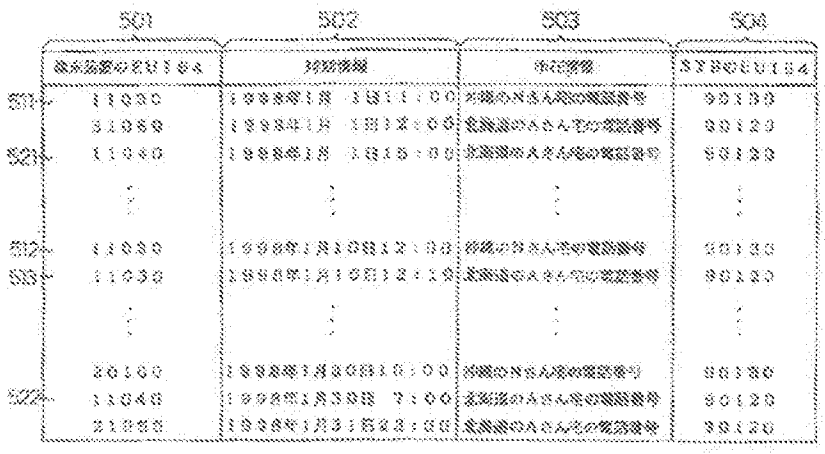
【図３】


管理装置 110
113
112
111
140
STB 120
213
114
116
118
STB 130

【図４】


管理装置 110
STB 120
213
111
813
811
812
STB 130

【図５】



【図８】

(a)

601

要求装置のEUI64	ゲスのEUI64
11030	90130
11030	90120

(b)

要求装置のEUI64	ゲスのEUI64
11030	90130

(c)

要求装置のEUI64	ゲスのEUI64
11030	90120

【図９】

(a)

901

要求装置のEUI64	ゲスのEUI64	参考
11030	90130	
31060	90120	
11040	90120	
21050	90120	
20160	90130	
30170	90130	

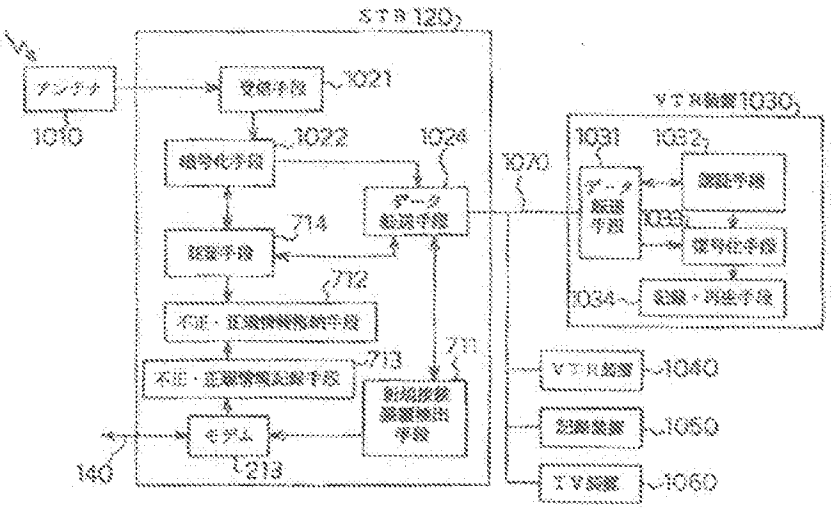
(b)

903

要求装置のEUI64	ゲスのEUI64	参考
11030	90130	本機
31060	90120	
11040	90120	
21050	90130	
20160	90130	
30170	90130	
11050	90130	本機

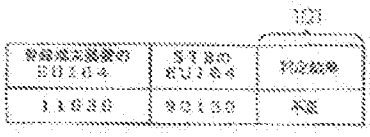
901
902

【図７】

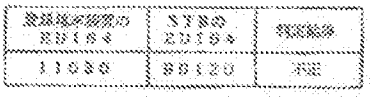


【図１０】

(a)



(b)

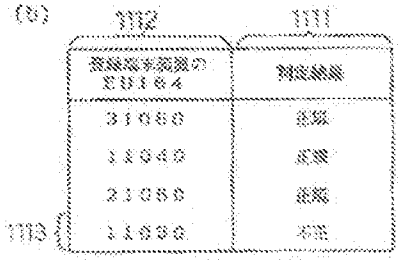


【図１１】

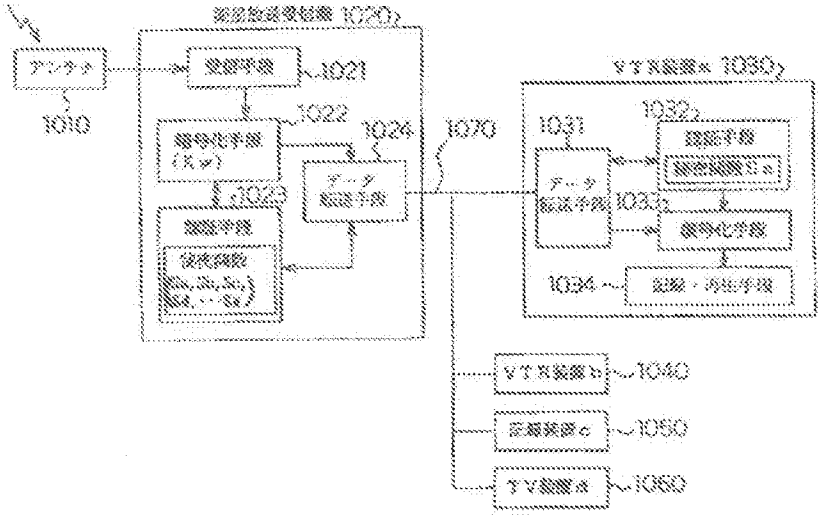
(a)

装置属性取得のID164	可否結果
31060	正規
11040	正規
21050	正規

(b)



【図12】



PATENT ABSTRACTS OF JAPAN

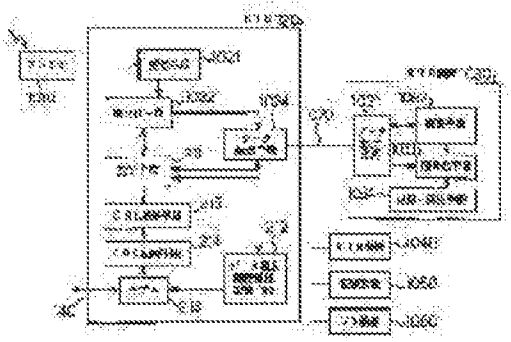
(11)Publication number : **11-232775**
(43)Date of publication of application : **27.08.1999**

(51)Int.Cl. G11B 20/10

(21)Application number : **10-031846**
(22)Date of filing : **13.02.1998**

(71)Applicant : **MATSUSHITA ELECTRIC IND CO LTD**
(72)Inventor : **YAMADA MASAZUMI**
IIZUKA HIROYUKI
TAKECHI HIDEAKI
GOTO SHOICHI

(54) CONTROL STANDARD MAKING METHOD, CONTROL STANDARD MAKING SYSTEM, AND MEDIUM



(57)Abstract:
PROBLEM TO BE SOLVED: To enable detecting an illegal terminal device before damage occurs more surely than conventional one.
SOLUTION: When data is required from a VTR device 1030 and the like having respective intrinsic EU 164 to STB 120, a certification means 211 performs certification based on the prescribed control standard about their data request, it is decided whether required data is transferred from STB 120 to the VTR device 1030 performing request or not in accordance with the certification result, and a data request history information storing means 212 sends data request history information including EU 164 of the VTR device to a control device 110 in accordance with the certification result. The control device discriminates whether the VTR device 1030 is a regular one or not by the prescribed discrimination standard utilizing the data request history information, makes CRL based on the certification result, and sends it to the SBT 120.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to a criteria-of-control preparation method, a criteria-of-control preparing system, and a medium.
[0002]
[Description of the Prior Art]A receiver for exclusive use receiving, and recording the TV program etc. which are sent by satellite broadcasting with the VTR devices connected to the receiver, or viewing and listening to them on television conventionally, is performed.
[0003]In this case, what record is forbidden, and the conditional data whose record is enabled only once are in the image and voice data broadcast. Therefore, in order to keep these conditions, it will be the requisite that recognize this condition correctly and the user side uses the device which operates regularly.
[0004]Then, when transmitting data recordable once from a receiver for exclusive use, for example to VTR devices, usually authentication operation for checking first whether the VTR devices are the above regular devices is performed. Data is not transmitted when it judges with it being an inaccurate device which performs operation which disregarded the above-mentioned conditions as a result of this authentication operation.
[0005]Hereafter, it is explained as the composition of the conventional exclusive receiver and a terminal unit focusing on the authentication operation, referring to drawing 12.
[0006]Drawing 12 is a block diagram showing the conventional junction state and composition of an exclusive receiver and a terminal unit.
[0007]As shown in the figure, the antenna 1010 is a means to receive the broadcasting electric-wave from a satellite.
The satellite broadcasting receiver (this is only hereafter called STB) 1020 is a means to change the broadcasting electric-wave which received into AV information.
The data-communications line 1070 is a bus line for the data communications in which STB1020 and each terminal unit described below were formed in between. moreover -- a terminal unit -- ****** -- VTR devices -- (-- A --) -- 1030 -- VTR devices -- (-- B --) -- 1040 -- a recorder -- (-- C --) -- 1050 -- furthermore -- TV -- a device -- (-- D --) -- data communications -- a line -- 1070 -- STB -- 1020 -- connecting -- having -- **** .
[0008]Next, the internal configuration of STB1020 is described further, referring to the figure.
[0009]That is, the reception means 1021 is a means to link directly with the antenna 1010, to restore to the received data, to cancel the scramble for broadcast given to the received data, and to separate the multiplexed received data further. The encoding means 1022 is a means to encipher the AV information outputted from the reception means 1021 by the work key Kw for the encryption which it had beforehand with a compression state. The encoding means 1022 is a means for enciphering the work key Kw using the sub key obtained from the authentication means 1023, and outputting the enciphered work key and the both sides of the AV information which enciphered [above-mentioned] to a terminal unit via the data input/output means 1024. It is because it is premised on recording that it is necessary to also send here the work key enciphered as mentioned above to a terminal unit after decrypting the transmitted AV information in a terminal unit. The authentication means 1023 is a means to perform authentication work using a predetermined secret function, and to generate the sub key corresponding to an attestation partner as the result in order to confirm mutually whether each other's both devices are regular devices between

the terminal units which have carried out the transfer request of AV information. The authentication means 1023 makes all the peculiar secret functions (Sa, Sb, Sc, Sd, .., Sn, ...) which all terminal units have correspond with those identification numbers, and holds them. The data transfer force means 1024 is IEEE1394 known as a digital interface. The data transfer means 1024 is a means to perform two transmission, isochronous transfer suitable for a data transfer like the image for which a real time nature guarantee is needed, or a sound, and assyncronous transfer suitable for transmission of data for attestation, a command, etc. without the necessity.

[0010]Next, the internal configuration of VTR devices (A) 1030 is described further.

[0011]The data transfer means 1031 is the same means as the data transfer means 1024 as shown in the figure.

It is a means to receive the enciphered work key and the enciphered AV information.

The authentication means 1032 has the peculiar secret function Sa beforehand.

It is a means to generate the sub key Ksa and to output to the decoding means 1033 as a result of authentication work.

The decoding means 1033 is a means to decrypt the enciphered work key which was obtained from the data transfer means 1031 by the sub key Ksa, and to decrypt the AV information which restored the work key Kw and was enciphered by the work key Kw. The record reproduction means 1034 is a means to record the decrypted AV information and to reproduce the record data.

[0012]in addition -- others -- a terminal unit -- it is -- VTR devices -- (-- B --) -- 1040 -- a recorder -- (-- D --) -- 1050 -- TV -- a device -- (-- D --) -- 1060 -- a record reproduction means -- removing -- the above -- VTR devices -- (-- A --) -- 1030 -- composition -- fundamental -- it is the same . However, the secret functions which each authentication means has beforehand will be Sb, Sc, and Sd, if it says in order of each above-mentioned device. Therefore, the sub keys generated by the authentication work of each device and STB1020 will be Ksb, Ksc, and Ksd, if it says in above order.

[0013]The contents of authentication work are described [in / next / the above composition] briefly.

[0014]For example, when performing the transfer request of AV information from VTR devices (A) 1030 to STB1020, in advance of the execution, the following authentication work is needed.

[0015]That is, first, the authentication means 1032 of VTR devices (A) 1030 generates the random number A1 and A2, and enciphers this with the secret function Sa. Here, the enciphered random number is indicated to be Sa (A1, A2). The authentication means 1032 transmits Sa (A1, A2) and the self identification number IDa to STB1020 via the data transfer means 1031 (Step 1001). Here, the identification number is beforehand given by the number peculiar to each terminal unit.

[0016]In STB1020, via the data transfer means 1024, the authentication means 1023 obtains Sa (A1, A2) and the identification number IDa, recognizes the identification number, and chooses the secret function Sa corresponding to it from two or more held secret functions (Step 1002). Thereby, the secret function which STB1020 should use for attestation between VTR devices (A) 1030 is specified.

[0017]Next, Sa (A1, A2) which the authentication means 1023 of STB1020 received [above-mentioned] using the secret function Sa is decoded, and the latter random number A2 is sent to VTR devices (A) 1030 among A1 restored and A2, without enciphering (Step 1003).

[0018]Next, the authentication means 1032 of VTR devices (A) 1030 compares A2 sent from STB1020 with the random number A2 which oneself generated at the above-mentioned step 1001. If both sides are in agreement, STB1020 can judge that it is a regular device (Step 1004).

[0019]Next, the authentication means 1023 by the side of STB1020 generates the random number B1 and B-2, and enciphers this with the secret function Sa. And Sa (B1, B-2) is transmitted to VTR devices (A) 1030 (Step 1005).

[0020]In VTR devices (A) 1030, Sa (B1, B-2) which the authentication means 1032 received [above-

mentioned] using the secret function Sa is decoded, and latter random number B-2 is sent to STB1020 among B1 and B-2s which were restored, without enciphering (Step 1006).
[0021]Next, the authentication means 1023 compares B-2 sent from VTR devices (A) 1030 with random number B-2 which oneself generated at the above-mentioned step 1005. If both sides are in agreement, it can be judged that VTR devices (A) 1030 are regular devices (Step 1007).
[0022]By the above, that both both sides are regular devices can check mutually, it comes, authentication work is completed, and transmission of the AV information to VTR devices (A) 1030 is permitted.
[0023]The four random numbers A1, A2, and B1 and B-2 exist in the authentication means 1023-1032 of both devices as a result of this authentication work. Then, next, both authentication means 1023-1032 generate the above-mentioned sub key Ksa using the random number A1 and B1, respectively. Since not using the random number A2 and B-2 has the circumstances where these were transmitted without enciphering, when generating a sub key, those who use the random number A1 without such the circumstances and B1 are because it sees from the safety of a key and excels more.
[0024]In the encoding means 1022, using the sub key Ksa generated by carrying out in this way, the work key Kw is enciphered and AV information is enciphered by the work key Kw. And the both sides of AV information Kw (AV) enciphered as the work key Ksa (Kw) enciphered [above-mentioned] are outputted to VTR devices (A) 1030 via the data input/output means 1024.
[0025]In VTR devices (A) 1030, the decoding means 1033 decodes the encryption work key Ksa (Kw) using the sub key Ksa obtained from the authentication means 1032, and decodes encryption AV information Kw (AV) using the decoded work key Kw.
[0026]
[Problem(s) to be Solved by the Invention]However, in the above authentication methods, an inaccurate person copies secret function Sn and the identification number IDn of a regular device as it is just as it is, When the inaccurate device which can perform the same authentication method as the above was manufactured and sold and the inaccurate device was used, in the above-mentioned authentication method, it has not detected that the device is an inaccurate device, and transmission of AV information was not able to be prevented.
[0027]Generally, in the unauthorized use by the 3rd person, such as a theft ATM card, direct damage occurs notably to the owner of the ATM card. Therefore, it is possible to prevent an unauthorized use promptly. On the other hand, as a receiving terminal device of broadcast data, even if the above inaccurate devices exist, there is peculiarity that damage to authorized personnel cannot surface easily. For example, even if it copies the data of copy prohibition unjustly, and it is rare that the concrete damage in which a royalty etc. are arrears surfaces and it surfaces, time most by it will have passed and it will also be expected that damage becomes serious.
[0028]Thus, in the conventional authentication method, since deer correspondence was not able to be performed after damage comes to light, it had the technical problem that it was imperfect as an authentication method.
[0029]An object of this invention is to provide the criteria-of-control preparation method, criteria-of-control preparing system, and medium which can ensure detection of an inaccurate device compared with the former in consideration of the technical problem of such a conventional method.
[0030]
[Means for Solving the Problem]When this invention according to claim 1 has a data request to a data transfer unit from each data request terminal unit which has a respectively peculiar identifier, about those data requests, As opposed to a data request terminal unit which performed attestation based on a predetermined attestation standard, and performed said data request from said data transfer unit according to a result of said attestation, Determine whether transmit the demanded data and a controlling device is

received from said data transfer unit according to a result of a usual state or said attestation, Send data request history information containing said identifier of the data request terminal unit, and said controlling device, It is a criteria-of-control preparation method which judges whether a data request terminal unit contained in the data request history information is regular, is based on the decision result, and creates or updates criteria of control by a predetermined judging standard using said data request history information sent.

[0031]This invention according to claim 5 a data transfer unit connected to each data request terminal unit which has a respectively peculiar identifier the singular number or a controlling device to manage [two or more], An identifier of a schedule connected newly or said data request terminal unit connected newly sent using new registration information to include by a predetermined judging standard. It is a criteria-of-control preparation method which judges whether a data request terminal unit corresponding to said new registration information is regular, is based on the decision result, and creates or updates criteria of control.

[0032]A criteria-of-control preparing system this invention according to claim 11 is characterized by that comprises the following.

Two or more data request terminal units which have a respectively peculiar identifier.

When a data request occurs from these data request terminal unit, about those data requests, performing attestation based on a predetermined attestation standard -- (1) -- to a data request terminal unit which performed said data request according to a result of the attestation, A data transfer unit which outputs data request history information which determines whether transmit the demanded data and contains said identifier of the data request terminal unit according to a result of (2) usual state or its attestation.

A controlling device which acquires said said outputted data request history information, judges whether a data request terminal unit contained in the data request history information by predetermined judging standard is regular, is based on the decision result, and creates or updates criteria of control.

[0033]

[Embodiment of the Invention]Below, an embodiment of the invention is described with reference to drawings.

[0034](A 1st embodiment) Drawing 1 is a lineblock diagram showing the composition of the criteria-of-control preparing system in the 1 embodiment of this invention, and it describes the composition of the criteria-of-control preparing system of this embodiment, referring to the figure below. In this embodiment, the same numerals were given to what was explained by drawing 12, and the thing of the fundamentally same composition, and the detailed explanation was omitted.

[0035]As shown in drawing 1, the controlling device 110 is a device which manages the 1STB120 which exists in every place, ..., the nSTB130, and each terminal unit. The controlling device 110 is a means to create and distribute the inaccurate device list of [for each STB to use in authentication work]. The telephone line 140 is a means to use for the data communications between the controlling device 110 and each STB120,130. this embodiment -- 1st STB120 -- A Mr. house in Hokkaido -- the -- nSTB assumes that it is provided in N Mr. house in Okinawa.

[0036]The terminal unit is connected to each STB120,130 on the data-communications line 1070, respectively. That is, VTR devices 1030, VTR devices 1040, the recorder 1050, and the TV device 1060 are connected to the 1STB120, and VTR devices 150, the recorder 160, and the TV device 170 are connected to the nSTB130 as shown in the figure. Here, suppose that VTR devices 150 are inaccurate devices. This inaccurate device shall be a device manufactured by injustice by copying the thing of regular VTR devices 1030 as it is just as it is as the license key mentioned later and EUI64.

[0037]These each terminal unit is provided with IEEE1394 as the data transfer means 1031 as drawing 12

explained it. In this embodiment, these terminal units are beforehand provided with EUI64 in IEEE1394 as a number peculiar to each device, i.e., an identification number, respectively. Here, EUI64 is a 64-bit identification code. These terminal units are provided with the license key corresponding to the identification number. Although this license key is a secret secret key given only to a regular terminal unit, the identification number of EUI64 is what is called an ID number that can be known also by whom on the occasion of data transfer etc. Hereafter, the identification number of EUI64 is only called EUI64 or an ID number. Peculiar EUI64 is provided also about each STB120,130. To each device, these identification numbers support the couple 1 and do not overlap.

[0038]Next, the internal configuration of STB120 is described in detail, referring to drawing 2.

[0039]In addition to the composition of the authentication means 1023 described by drawing 12, STB120 is provided with the data request history information storage means 212, the modem 213, the CRL recording device 214, and the CRL storing means 215 as shown in drawing 2.

[0040]The authentication means 211 are a point provided with the service key formation function which can make the service key which is the same key as a license key, and a point which takes into consideration the list of the inaccurate device mentioned later in attestation, and are different from the authentication means 1023 described by drawing 12. This service key formation function is a function which generates a service key from EUI64 (ID number) obtained from the terminal unit. Therefore, the authentication means 211 does not need to memorize EUI64 of a terminal unit beforehand.

[0041]The data request history information storage means 212 is a means to generate the hysteresis information about the data request, and to memorize through the authentication work mentioned later each time about what transmission of requested data completed, when the data transfer request of a predetermined program occurs from a terminal unit. This data request history information comprises EUI64 of the terminal unit which carried out the data transfer request, time information which specifies time with the data request from that terminal unit, and location information which specifies the whereabouts of that terminal unit. The data request history information storage means 212 acquires these EUI(s) information - location information from the authentication means 211. The data request history information storage means 212 accumulates such hysteresis information from each terminal unit of one-month Hazama, and is a means sent to the controlling device 110 via the modem 213 for every month.

[0042]The CRL recording device 214 is a means which obtains the list data for which the inaccurate device sent from the controlling device 110 was indicated from the modem 213, and is recorded and updated at the CRL storing means 215. The CRL storing means 215 is a memory means for storing the list data of an inaccurate device. In this specification, the list of an inaccurate device is only called CRL (Certification Revocation List). The criteria of control of this invention according to claim 1 correspond to CRL.

[0043]Next, the internal configuration of the controlling device 110 is described in detail, referring to drawing 3.

[0044]The history information storage means 112 is a means to make each data request history information transmitted for every month from each STB120,130 at the period correspond with EUI64 of STB of a transmitting agency, and to memorize it temporarily via the modem 111 as shown in drawing 3. The unjust device determining means 113 in all the data request history information for one month from each STB memorized by the above-mentioned history information storage means 112, When two or more EUI64 [same] exist, it is a means to determine the data request terminal unit which compares the time information and location information corresponding to EUI64 of these plurality, respectively, and has EUI64 with an unjust possibility. The CRL preparing means 114 is a means to obtain the above-mentioned decision results outputted for every month from the unjust device determining means 113, to create the list of an inaccurate device, and to output. All the CRL memory measures 115 are means to obtain the list data

from the CRL preparing means 114, to make addition of a new inaccurate device, correction of data, etc. to the already accumulated list, and to memorize all the CRL(s) about the terminal unit of all the areas. The individual CRL preparing means 116 is a means to transmit to STB which creates individual CRL corresponding to each STB, and corresponds via the modem 111. Individual CRL is a list of the inaccurate device packed for every STB, and is not created about STB from which the inaccurate device is not detected.

[0045]Mainly referring to drawing 4 - drawing 6 (c), operation of this embodiment is described and the 1 embodiment which starts the criteria-of-control preparation method of this invention simultaneously is also described [in / next / the above composition]. Drawing 4 is a figure to explain the memory content of the data request history information storage means 212 in STB120 from January 1, 1997 to the 31st of the same month, and drawing 5, It is a figure explaining the memory content of the history information storage means 112 in the controlling devices from January 1, 1997 to the 31st of the same month.

[0046]Here, as of January 31, 1997, to CRL (list of an inaccurate device) of the CRL storing means 215 of STB120, the inaccurate device is not yet indicated, i.e., it presupposes at it that it is in an empty situation. It is sky condition also about CRL of the CRL storing means of STB130.

[0047]First, explanation here describes the authentication operation using CRL in (1) STB, next describes creation of CRL in (2) controlling devices, and distribution of CRL to STB, and states the updating operation of CRL in (3) STB to the last.

(1) Authentication operation using CRL in STB : here, when STB120 receives the transfer request from VTR devices 1030 which are regular devices about the AV information of the program which received by the reception means 1021, for example, perform the following authentication operation. This transfer request satisfies the demand which suited at 12:10 a.m. on January 10, Heisei 10 in the hysteresis information indicated in drawing 4 and drawing 5.

[0048]Step 1: The authentication means 211 of STB120 obtains first EUI64 (here, they may be No. 11030) of VTR devices 1030 which have carried out the transfer request from the data transfer means 1024.

[0049]Step 2: and the authentication means 211 confirm whether the same number as the EUI64 is registered in CRL as a number of an inaccurate device with reference to CRL of the CRL storing means 215. At this time, since CRL is sky condition as above-mentioned, the decision result of being unregistered comes out and that EUI64 goes into full-scale authentication work (Step 3). If a judgment that it registers with CRL comes out in this check stage, subsequent authentication work will not be performed and a data transfer with a demand will not be performed, either.

[0050]Step 3: The authentication means 211 generates a service key from a service key formation function using EUI64 of VTR devices 1030 obtained at Step 1. Thus, the generated service key is the same key as the license key which VTR devices 1030 have. A license and a service key correspond to the secret function Sa described by drawing 12.

[0051]On the other hand, VTR devices 1030 perform the same authentication work as what was already explained by drawing 12 by both Hazama using the license key which it has beforehand using the service key which carried out the authentication means 211 in this way, and was generated. That is, both devices generate the same sub key Ksa using the random number A1 and B1, respectively.

[0052]Step 4: The encoding means 1022 enciphers the work key Kw using the above-mentioned sub key Ksa, and enciphers AV information using the work key Kw, and transmits the encryption data (Ksa (Kw), Kw (AV)) of these both sides to VTR devices 1030.

[0053]Supposing it is a process of this attestation and EUI64 sent from the terminal unit is a completely random number which does not have the correspondence relation beforehand determined as the license key which that terminal unit has, for example, The key generated by the service key formation function

stops being in agreement with the license key. because, a service key formation function -- the account of the upper -- it is because it is constituted based on the correspondence relation defined beforehand so that a service key may be generated from EUI64. Therefore, the data transfer which the above-mentioned attestation on condition of the key which both devices have in this case being the same stops having materialized, and was demanded in this case is not performed.

[0054]Step 5 : the data request history information storage means 212, From the authentication means 211 as EUI64 of VTR devices 1030 which are the destination about what data transfer completed at Step 4, As No. 11030 and time information with a demand, each information at 12:10 a.m. on January 10, Heisei 10 is acquired, and it records as data request history information (refer to drawing 4). Here, the statement of drawing 4 is explained. Namely, No. 31060 as each number written in the column 401 of EUI64 of a terminal unit in the figure, No. 11040, No. 11030, and No. 21050, Sequentially from before, EUI64 of the TV device 1060, VTR devices 1040, VTR devices 1030, and the recorder 1050 is shown.

[0055]Step 6: Whenever a data transfer request occurs from each terminal units 1030-1060, perform the above-mentioned steps 1-5 like the above. And the data request history information storage means 212, To each historical data (refer to drawing 4) by which record accumulation was carried out in one month, it is EUI64 (here) of STB120.And you consider it as No. 90001, let what attached the telephone number as the location information be data request history information (it transmits to the controlling device 110 for every month via the telephone line 140 from the modem 213.).

(2) Creation of CRL in a controlling device, and distribution operation of CRL to STB : here, describe operation of the controlling device 110.

[0056]Step 101: The data request history information mentioned above for every month is transmitted to the history information storage means 112 of the controlling device 110 via the modem 111 from STBs 120-130 of every place. The history information storage means 112 holds these information as hysteresis information.

[0057]Step 102: The unjust device determining means 113 acquires the hysteresis information held at the history information storage means 112, and rearranges a data content into time order by the time information (refer to drawing 5). Drawing 5 is a figure for explaining the contents of the rearranged hysteresis information.

[0058]And if there is what has EUI64 [same] of the terminal unit shown in the column 501 (refer to drawing 5) of EUI64 of a terminal unit, the time information and location information corresponding to them will be compared, respectively, and the terminal unit corresponding to EUI64 with an unjust possibility will be determined.

[0059]That is, when shown in drawing 5, all EUI64 of the terminal unit indicated in each line to which the numerals 511,512,513 were given are No. 11030. Then, these are checked first. When the time information of the line to which the numerals 511 and 512 were given is compared, it is a history of the transfer request in time different, respectively, and it can be judged that there is no inconsistency in both histories. However, it is shown that the situation which is contradictory to the premise of not existing has generated the device which has EUI64 with two same histories indicated in the line which attached the numerals 512 and 513. The number 90002 written in the column 504 of EUI64 of STB of drawing 5 is EUI64 of STB130.

[0060]Namely, when the unjust device determining means 113 compares the data of the column 502 of the time information of these both sides, and the column 503 of location information, it is a 10-minute [after the place where one side calls it Okinawa and another side is called Hokkaido and which was left distantly geographically] difference, It sees from the fact that there was a transfer request with the device which has the EUI64 [same], and the device which has the EUI64 [same] judges that it exists in A Mr. house in Hokkaido, and N Mr. house in Okinawa. And the both sides of the device of these both sides consider

that the unjust device determining means 113 is an inaccurate device, and it sends the decision result to the CRL preparing means 114. Although VTR devices 150 currently installed in N Mr. house in Okinawa are actually inaccurate devices, since it does not understand, in this stage, it considers that both sides are inaccurate for the time being till the place which says any are actually inaccurate devices. That judgment with unjust any is mentioned later. The situation which is contradictory to the premise that the device which has the EUI64 [same] from the result of having compared the historical data indicated in the line which attached the numerals 521,522 does not exist is not found.

[0061]Step 103: From the decision result obtained from the unjust device determining means 113, the CRL preparing means 114 creates CRL as shown in drawing 6 (a), and sends it to all the CRL memory measures 115. Such creation operation of CRL is performed every month, and it memorizes at all the CRL memory measures 115 at every time. Therefore, with the list sent from the CRL preparing means 114, all the CRL memory measures 115 add an addition, correction, etc. to already memorized CRL, and update them each time.

[0062]Step 104: The individual CRL preparing means 116 separates the contents of the CRL for every STB, seeing the column 601 of EUI64 of STB in CRL created by the CRL preparing means 114. Drawing 6 (b) and (c) is individual CRL created, respectively in order to distribute to STB130 and STB120. The individual CRL preparing means 116 distributes these individual lists to corresponding STB via the modem 111.

(3) Updating operation of CRL in STB : STB120 which obtained individual CRL (refer to drawing 6 (c)) distributed from the controlling device 110 performs the following operations.

[0063]Step 201:214, i.e., a CRL recording device, obtains the above-mentioned individual CRL from the modem 213, and it records it on the CRL storing means 215 which was sky condition till then. Thereby, connection, now VTR devices 1030 (EUI64 is No. 11030) which are are registered into the CRL storing means 215 by STB120 as an inaccurate device. Therefore, since it becomes clear in the stage of the above-mentioned step 2 that it is an inaccurate device even if the data transfer request from these VTR devices 1030 will occur from now on, there is no data transfer limping gait ******. Thereby, expansion of the damage caused by an inaccurate device can be prevented. Also in STB130, same operation is completely performed. In this case, VTR devices 150 (EUI64 is No. 11030) are registered into the CRL storing means of STB130 as an inaccurate device.

[0064](A 2nd embodiment) Drawing 7 and 8 are the lineblock diagrams showing the composition of STB and the controlling device which constitute the criteria-of-control preparing system in the 1 embodiment of this invention, and they describe the composition of the criteria-of-control preparing system of this embodiment, referring to the figure below. In this embodiment, the same numerals were given to what was explained by a 1st embodiment, and the thing of the fundamentally same composition, and the detailed explanation was omitted. The composition of the whole system of this embodiment is the same as what was fundamentally described by drawing 1.

[0065]The main points of difference between this embodiment and the above-mentioned embodiment are the processes of creation of the injustice and regular determination information about a terminal unit. Therefore, it explains focusing on this point of difference here. The criteria of control of this invention according to claim 5 correspond to injustice and regular determination information.

[0066]The main points which are different from the composition shown by drawing 2 in the composition of STB120 shown in drawing 7. The new contact detection means 711, injustice and a regular information storing means 712, and injustice and a regular information storage means 713 are provided instead of the data request history information storage means 212 of drawing 2, the CRL storing means 215, and the CRL recording device 214. Unlike what was described by a 1st embodiment, the authentication means 714 does not have composition which outputs the hysteresis information about the data transfer request from a

terminal unit. Other composition is the same.
[0067]The new contact detection means 711 is a means to detect it and to acquire the EUI64, when there is a device newly connected to the data-communications line 1070 of STB120. EUI64 acquired attaches EUI64 of STB120 and is sent to the controlling device 110 from the modem 213. This operation is the work for the new registration to the controlling device of the newly connected device, and is also the work for checking simultaneously whether that new contact is inaccurate. Since this operation is performed in the case of new registration, unlike what is performed to the degree of the data transfer request described by a 1st embodiment of the above, it is first-time operation.
[0068]Injustice and the regular information storage means 713 are means to store in injustice and the regular information storing means 712 the information sent from the controlling device 110.
[0069]Next, the composition of the controlling device 110 is described, referring to drawing 8.
[0070]As shown in the figure, the inquiry means 811 obtains EUI64 of the terminal unit which is sent from STBs 120-130 and which was newly established as new registration information, and EUI64 of STB of the transmitting origin, and is a means to judge whether it is inaccurate. The new registration device list information memory measure 812 is a means to memorize EUI64 of the new registration device obtained from the inquiry means 811.
[0071]Injustice and the regular determination information preparing means 813 are means to create whether to be inaccurate and that regular determination information about the device which had new registration from the above-mentioned checked result by the inquiry means 811, and to transmit which the information to corresponding STB via the modem 111. When it becomes double registrations, injustice and the regular determination information preparing means 813 consider that the device of the both sides which have the EUI64 is an inaccurate device, and creates and distributes the list corresponding for every STB of unjust information (refer to drawing 6 (b) and (c)).
[0072]Mainly referring to drawing 9 (a) - drawing 10 (b), operation of this embodiment is described and the 1 embodiment which starts the criteria-of-control preparation method of this invention simultaneously is also described [in / next / the above composition]. VTR devices 1040 shown in drawing 1 by this embodiment on account of explanation, the recorder 1050, and the TV device 1060, finishing [connection with STB120] already -- it is -- finishing [VTR devices 150, the recorder 160, and the TV device 170 / connection with STB130] already -- it is -- it is assumed that ** and the new registration explained below have also ended just to these terminal units. VTR devices 1030 presuppose that it is a device newly connected to STB120. VTR devices 150 presuppose that it is an inaccurate device as the above-mentioned embodiment also explained them. Explanation here describes first the detecting operation of the device connected newly in (1) STB, Next, the authentication operation which used the renewal of injustice and regular determination information, and the injustice and regular determination information in (3) STB for the last about creation of the new registration, and the injustice and regular determination information in (2) controlling devices, etc. is described. These explanation is given focusing on a point of difference with a 1st embodiment.
(1) Operation in STB ; suppose that VTR devices 1030 were newly connected to STB120 as above-mentioned (refer to drawing 7).
[0073]Step 201: The new contact detection means 711 shown in drawing 7 reads periodically EUI64 of all the terminal units connected to the data-communications line 1070, and records it on the memory (graphic display abbreviation) to build in. And it compares with the newest record data of EUI64 of the terminal unit already recorded.
[0074]In the situation where VTR devices 1030 were newly connected, the periodical thing of above-mentioned EUI64 it read and the device of No. 11030 was newly connected [the thing] for EUI64 by the above-mentioned comparison operations is detectable.

[0075]Step 202: The new contact detection means 711 transmits to the controlling device 110 via the modem 213 further by making into new registration information EUI64 (No. 11030) of the device which is the target of the new registration detected [above-mentioned], and EUI64 (No. 90120) of STB120 of a transmitting agency.
(2) Operation in a controlling device : drawing 9 (a) is a figure for explaining the memory content of the new registration device list information memory measure 812 before registering VTR devices 1030, and drawing 9 (b) is the figure after VTR devices 1030 were registered. It explains referring to these drawings.
[0076]Step 301: Based on the new registration information transmitted from SBT120, the inquiry means 811 shown in drawing 8 investigates the memory content (refer to drawing 9 (a)) of the new registration device list information memory measure 812, and confirms whether the registration produces the situation of double registrations. EUI64 contained in new registration information is No. 11030, and this already overlaps with a registered thing (the numerals 901 were attached among drawing 9 (a)) as it shows drawing 9 (a). Therefore, about EUI64 of the duplicate both sides, the inquiry means 811 judges with it being inaccurate, and outputs.
[0077]Step 302: The new registration device list information memory measure 812 registers the contents of the new registration information sent from the inquiry means 811 (the numerals 902 were attached among the figure).The information on an unjust purport is recorded on the remarks column 903 about EUI64 of the duplicate both sides from the above-mentioned decision result. The judgment of any are really inaccurate is mentioned later.
[0078]Step 303: Injustice and the regular determination information preparing means 813 create the list of injustice and regular determination information as shown in drawing 10 (a) and (b) from the decision result sent from the inquiry means 811. These lists are packed for every STB. The information which shows injustice is recorded on the column 101 of the decision result by drawing 10 (a) and (b) as above-mentioned. However, when judged with it being regular as a result of the judgment of the new registration information by the inquiry means 811 in Step 301, the information which shows a norm needless to say is recorded on the column 101 of a decision result.
[0079]Step 304: Injustice and the regular determination information preparing means 803 transmit the individual list of decision results created as mentioned above to STB120 and STB130 via the modem 111. This transmission is performed whenever the new registration information mentioned above is sent from STB.
[0080](3) Operation in STB : drawing 11 (a) is a figure showing the contents already stored in injustice and the regular information storing means 712, and shows the situation before transmitting the individual list of decision results shown in drawing 10 (a). Drawing 11 (b) shows the situation after the contents of the individual list of decision results shown in drawing 10 (a) were reflected.
[0081]The injustice and the regular information storage means 713 shown in drawing 7 obtain the individual list of decision results transmitted from the controlling device 110 from the modem 213, and adds it to the contents of record shown in drawing 11 (a). The contents of the above-mentioned individual list are added to the 4th line (the numerals 1113 were attached among the figure) from on drawing 11 (b). The column 1111 of the decision result of the figure shows whether the device shown in the column 1112 of EUI64 of a registering terminal device is inaccurate or regular.
[0082]On the other hand, also in STB130, the completely same operation as the above is performed.
[0083]Next, the case where there is a transfer request of AV information is described from VTR devices 1030 to STB120.
[0084]In this case, in the authentication operation described at Step 1 described by a 1st embodiment - Step 4, since only the contents of the above-mentioned step 2 differ, only that point of difference is described.

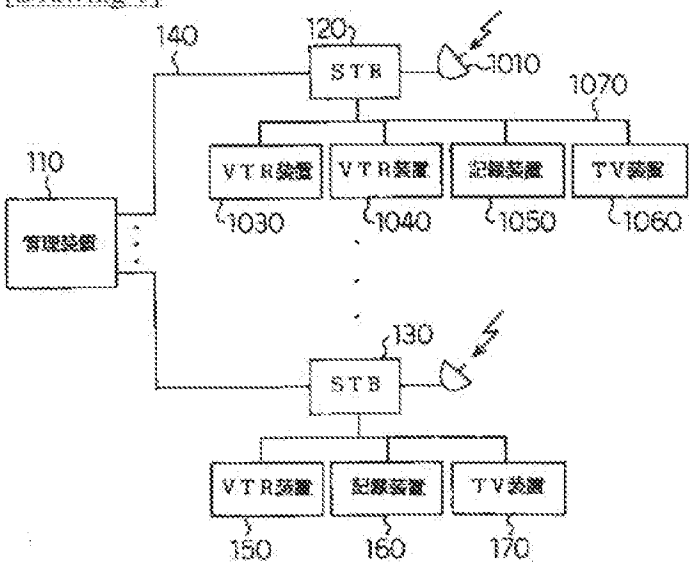
[0085]That is, the authentication means 714 confirms whether EUI64 of the terminal unit which advanced the transfer request is regular or inaccurate with reference to injustice and the regular information storing means 712 after the same operation as the above-mentioned step 1. According to the information recorded on the line which attached the numerals 1113, it is shown that EUI64 which has carried out the above-mentioned transfer request is unjust as for the device of No. 11030 as shown in drawing 11 (b). Therefore, the authentication means 714 does not perform subsequent authentication work, and does not perform a data transfer with a demand, either.
[0086]As a result of a check, when regular, the same operation as the contents described at the above-mentioned steps 3-4 is performed.
[0087]When EUI64 of a device with a transfer request is unregistered to injustice and the regular information storing means 712, it directs that the authentication means 714 sends the new registration information on the device of the demand origin to the controlling device 110 to the new contact detection means 711. Thereby, expansion of the damage caused by an inaccurate device can be prevented.
[0088]By the way, it is **** about the judgment of the any when it is judged with both devices being inaccurate as mentioned above, are really inaccurate.
[0089]In this case, since the user who did not have the data which it was considered by STB that it was inaccurate and was demanded transmitted tumefies doubt of the device which received that unjust judging, he can request investigation from the control center which owns the controlling device 110. The control center which received the investigation request investigates the truth of the device, and confirms certainly whether be what was manufactured or converted by the inaccurate method. And if it turns out to be regular, the data currently recorded on the controlling device will be corrected and the correcting result will be transmitted to applicable STB. A transfer request will be accepted to the device which turned out to be regular by this.
[0090]A magnetic recording medium, an optical recording medium, etc. which recorded the program for making a computer perform any of the embodiment described above or all or a part of steps (MEANS) of each steps (or means) of one statement can be created, and the same operation as the above can also be performed using this. The same effect as the above is demonstrated also in this case.
[0091]Although the above-mentioned embodiment described the case where it recorded on the data request history information storage means 212 for all the data transfer requests which occurred from the terminal unit, the composition recorded only for the transfer request of not only this but data important for example, may be used. Here, it is paper Lec (PREC) and data like pay-per-view (PPV) of charging as important data, for example if it records. Therefore, what pays money for every chain flannel, for example, the program data of a free channel, etc. are good also as outside of an object.
[0092]Although a 2nd embodiment of the above described the case where it was detected automatically that the terminal unit was newly connected, the registration postcard is attached not only to this but to the device purchased newly, for example, and it is good also as composition with which a user sends the postcard to the control center which owns a controlling device.
[0093]Although the above-mentioned embodiment described the case where transmission to STB of CRL, or injustice and regular information was performed using a telephone line, it may send not only by this but by broadcast.
[0094]Although a 2nd embodiment of the above compared the new registration information sent from the STB side, and the already sent accumulation data of new registration information and described the case where it checked for no duplication, It may have a memory holding the list data of EUI64 of a produced regular device indicated to the production information led from each company which manufactured not only this but the device, and the composition of also performing comparison with the contents of the memory may be used in the case of the above-mentioned comparison. Even when EUI64 contained in new

registration information is completely random, by comparing with the contents of the above-mentioned memory, If it is a number which does not correspond, it is not recorded on the new registration device list information memory measure 812 even if, but even if it is in the situation not overlapping, it can judge with it being inaccurate and the effect of dishonesty prevention will improve more.
[0095]The above-mentioned embodiment is available even for even referring to not only this but only referring to CRL as for example, contents of attestation, or injustice and regular information, although the case where full-scale authentication operation was performed was described.
[0096]Using a computer, work of a program may realize by software or the processing operation of each means of the above-mentioned embodiment may realize the above-mentioned processing operation in hard by circuitry characteristic for not using a computer.
[0097]The data transfer unit of the invention in this application was STB in the above-mentioned embodiment, when the STB detected connection with STB of the data request terminal unit connected newly, it explained the case where the new registration information on the data request device was transmitted to a controlling device, but. Not only in this, for example, the new contact detection means 711, If there is nothing same as compared with EUI64 of the terminal unit which obtains EUI64 of the VTR devices 1030, already checks new connection, and is recorded when attestation is newly required from VTR devices 1030, The composition detected as what was connected newly may be sufficient as the VTR devices 1030.
[0098]By the above-mentioned embodiment, when it has been checked as a result of attestation that it is a regular device, explained the example of sending the data request history information which contains the identifier (EUI64) of the data request terminal unit from a data transfer unit (STB) to a controlling device, but. It may not be concerned with the result of not only this but attestation, but the composition of sending the data request history information may be used to a controlling device. In this case, what is necessary is just to send with hysteresis information also that, when it becomes clear that it is an inaccurate device in process of attestation.
[0099]Although the above-mentioned embodiment described the case where STB used the criteria of control (CRL, or injustice and regular determination information) of the invention in this application in authentication operation, the composition which uses neither the above CRL, nor injustice and regular determination information in the authentication operation not only as this but as an STB may be used.
[0100]
[Effect of the Invention]This invention has the strong point in which detection of an inaccurate device can be ensured compared with the former so that clearly from the place described above.

[Translation done.]

DRAWINGS

[Drawing 1]

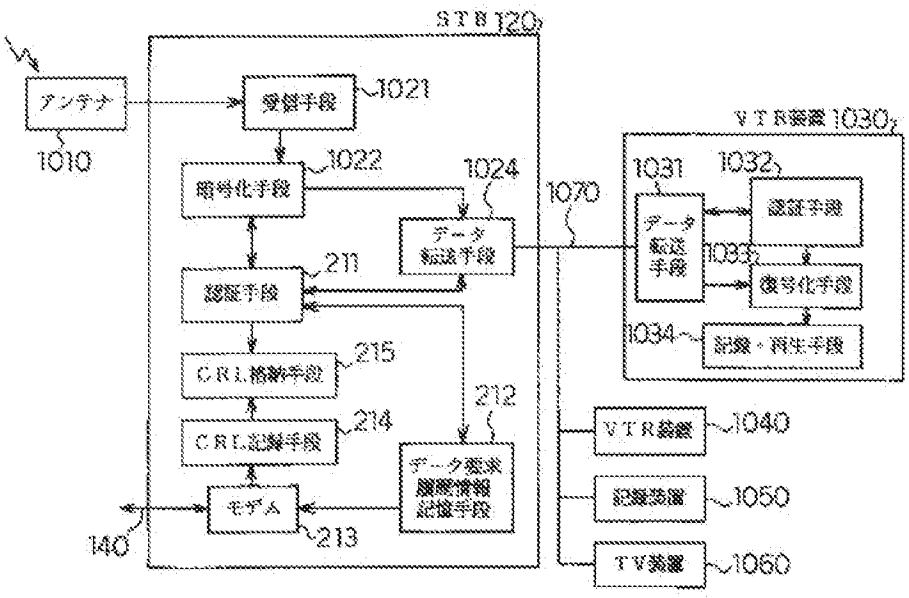


[Drawing 4]

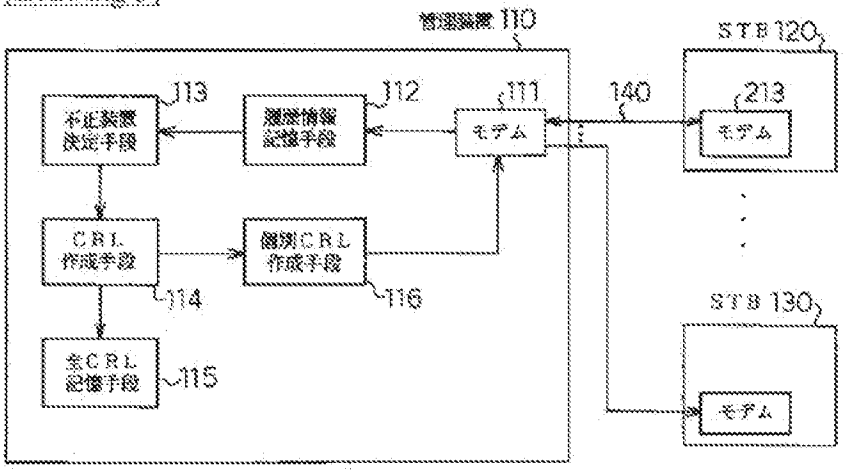
401

端末装置のEUI64	時刻情報
31060	1998年1月 1日12:00
11040	1998年1月 1日15:00
⋮	⋮
11030	1998年1月10日12:10
⋮	⋮
11040	1998年1月30日 7:00
21050	1998年1月31日23:00

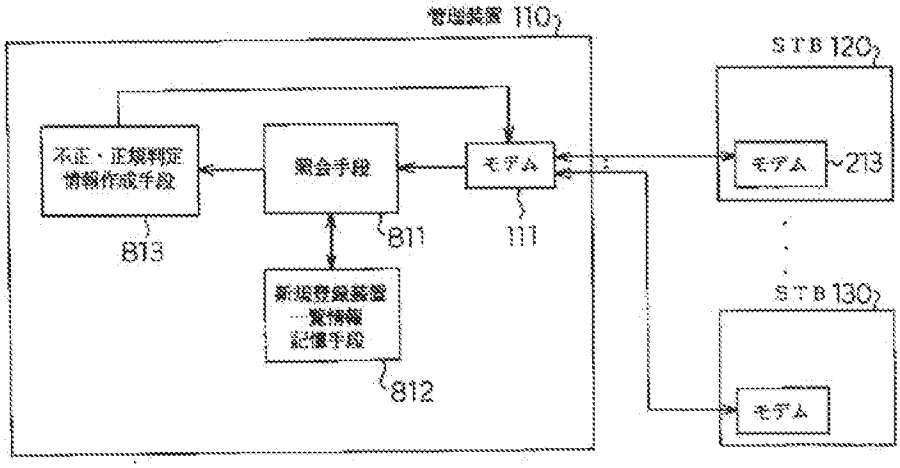
[Drawing 2]



[Drawing 3]



[Drawing 8]



[Drawing 5]

	501	502	503	504
	端末装置のEUI64	時刻情報	宛先情報	STBのEUI64
511	11030	1998年1月 1日11:00	沖縄のNさん宅の電話番号	90130
	31060	1998年1月 1日12:00	北海道のAさん宅の電話番号	90120
521	11040	1998年1月 1日15:00	北海道のAさん宅の電話番号	90120
	⋮	⋮	⋮	⋮
512	11030	1998年1月10日12:00	沖縄のNさん宅の電話番号	90130
513	11030	1998年1月10日13:10	北海道のAさん宅の電話番号	90120
	⋮	⋮	⋮	⋮
	30160	1998年1月30日10:00	沖縄のNさん宅の電話番号	90130
522	11040	1998年1月30日 7:00	北海道のAさん宅の電話番号	90120
	21050	1998年1月31日23:00	北海道のAさん宅の電話番号	90120

[Drawing 6]

(a)

	601
端末装置のEUI64	STBのEUI64
11030	90130
11030	90120

(b)

端末装置のEUI64	STBのEUI64
11030	90130

(c)

端末装置のEUI64	STBのEUI64
11030	90120

[Drawing 9]

(a)

901

登録端末装置のEUI64	STBのEUI64	備考
11030	90130	
31060	90120	
11040	90120	
21050	90120	
20160	90130	
30170	90130	

(b)

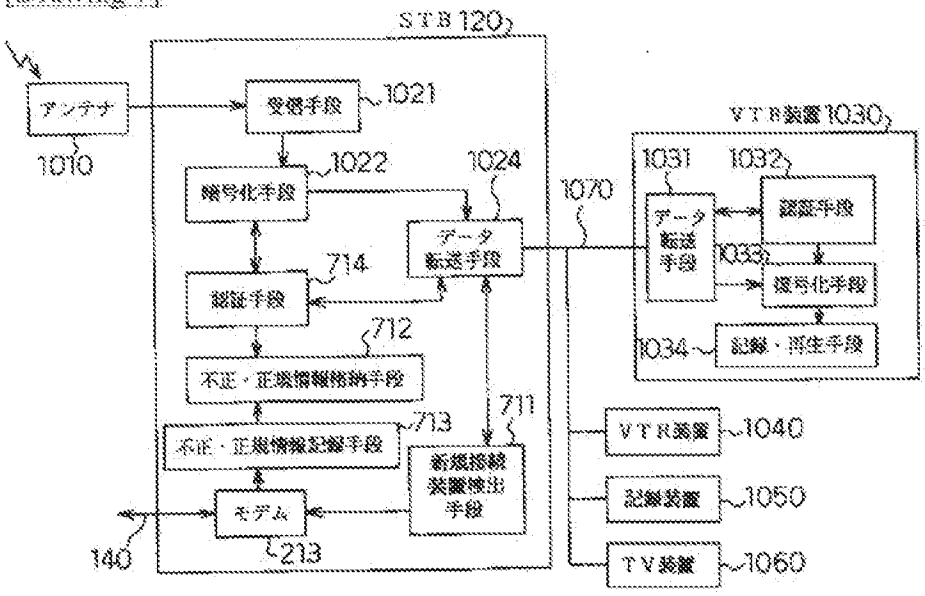
903

901

902

登録端末装置のEUI64	STBのEUI64	備考
11030	90130	不正
31060	90120	
11040	90120	
21050	90120	
20160	90130	
30170	90130	
11030	90120	不正

[Drawing 7]



[Drawing 10]

(a)

101

登録端末装置のEUI64	STBのEUI64	判定結果
11030	90130	不正

(b)

登録端末装置のEUI64	STBのEUI64	判定結果
11030	90120	不正

[Drawing 11]

(a)

登録端末装置のEUI64	判定結果
31060	正規
11040	正規
21050	正規

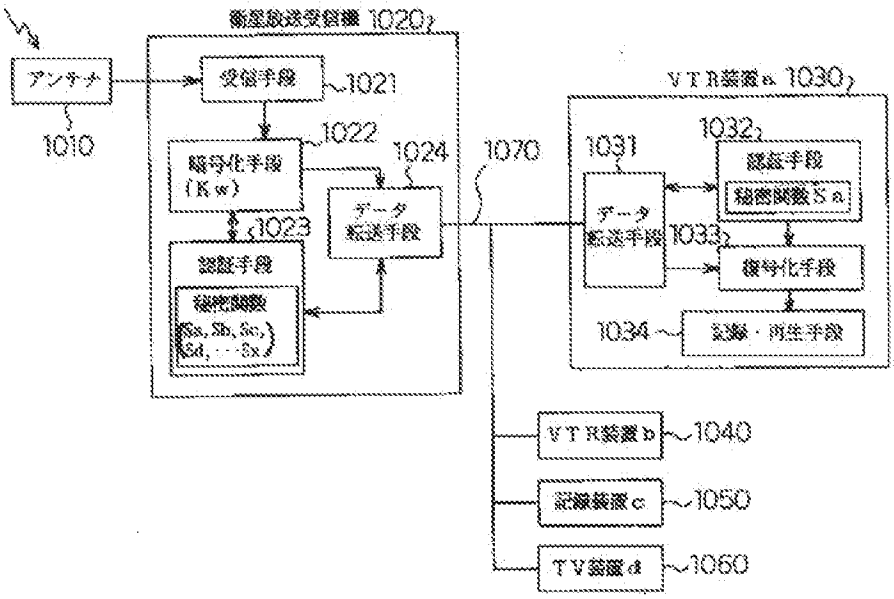
(b)

1112 1111

登録端末装置のEUI64	判定結果
31060	正規
11040	正規
21050	正規
11030	不正

1113

[Drawing 12]



[Translation done.]

CLAIMS

[Claim(s)]
[Claim 1]When a data request occurs to a data transfer unit from each data request terminal unit which has a respectively peculiar identifier, about those data requests, As opposed to a data request terminal unit which performed attestation based on a predetermined attestation standard, and performed said data request from said data transfer unit according to a result of said attestation, Determine whether transmit the demanded data and a controlling device is received from said data transfer unit according to a result of a usual state or said attestation, Send data request history information containing said identifier of the data request terminal unit, and said controlling device, A criteria-of-control preparation method judging whether a data request terminal unit contained in the data request history information is regular, being based on the decision result, and creating or updating criteria of control by a predetermined judging standard using said data request history information sent.
[Claim 2]Are information characterized by comprising the following and said predetermined judging standard in said controlling device, In all the data request history information transmitted from said two or more data transfer units, The criteria-of-control preparation method according to claim 1 being what determines a data request terminal unit which compares said time information corresponding to an identifier and said location information of these plurality, respectively, and has an identifier with an unjust possibility when two or more same identifiers exist.
Time information which specifies time with said data request from said data request terminal unit with which a group formed by a data request terminal unit and said data transfer unit of said plurality has those with two or more groups, and said data request history information has the identifier other than said identifier.
Location information which specifies the whereabouts of the data request terminal unit.

[Claim 3]When a data request terminal unit which has an identifier with a decision result by said judging standard and said unjust possibility is determined, consider that all the data request terminal units which have the identifier same in them are inaccurate things, and as said criteria of control, The criteria-of-control preparation method according to claim 2 creating or updating an unjust list of data request terminal units it was considered that were these inaccurate things.
[Claim 4]The criteria-of-control preparation method according to claim 3, wherein said controlling device transmits said all or some of unjust list to said data transfer unit and said data transfer unit performs said attestation, using said transmitted unjust list at least.
[Claim 5]A data transfer unit connected to each data request terminal unit which has a respectively peculiar identifier the singular number or a controlling device to manage [two or more], An identifier of a schedule connected newly or said data request terminal unit connected newly sent using new registration information to include by a predetermined judging standard, A criteria-of-control preparation method judging whether a data request terminal unit corresponding to said new registration information is regular, being based on the decision result, and creating or updating criteria of control.
[Claim 6]A group formed by a data request terminal unit and said data transfer unit of said plurality those with two or more groups, and said data transfer unit, When connection with said data transfer unit of said data request terminal unit connected newly is detected, Transmit new registration information on the data request device to said controlling device, and said predetermined judging standard, The same identifier as an identifier contained in the new registration information whenever said new registration information is transmitted, The criteria-of-control preparation method according to claim 5 being a standard which

judges whether it has already existed in a list of said identifiers currently transmitted and held from said two or more data transfer units.
[Claim 7]When a decision result by said judging standard shows that said same identifier exists during said list, consider that all the data request terminal units which have the identifier same in them are inaccurate things, and as said criteria of control, The criteria-of-control preparation method according to claim 6 creating or updating unjust information on a data request terminal unit it was considered that were these inaccurate things.
[Claim 8]a decision result by said judging standard -- (1) -- it considering that all the data request terminal units which have the identifier same in them are inaccurate things, and as said criteria of control, when it is shown that said same identifier exists during said list, Unjust information on a data request terminal unit it was considered that were these inaccurate things is created, or -- updating -- (2) -- it considering that a data request terminal unit which has said identifier contained in said new registration information is a regular thing, and as said criteria of control, when it is shown that said same identifier does not exist during said list, The criteria-of-control preparation method according to claim 6 creating or updating regular information on a data request terminal unit it was considered that was the regular thing.
[Claim 9]Said controlling device transmits to said data transfer unit, and said all or a part of unjust information, or said regular information said data transfer unit, When a data request occurs from each data request terminal unit, about those data requests, The criteria-of-control preparation method according to claim 8 being what determines whether transmit the demanded data to a data request terminal unit which attested using said transmitted unjust information or regular information at least, and performed said data request according to the authentication result.
[Claim 10]When said controlling device transmits said a part of unjust information to said data transfer unit, The criteria-of-control preparation method according to claim 4 or 9 which extracts information corresponding to the data transfer unit and a data request terminal unit in connecting relation among information about a data request terminal unit currently mentioned to said unjust information, and is characterized by transmitting.
[Claim 11]A criteria-of-control preparing system comprising:
Two or more data request terminal units which have a respectively peculiar identifier.
When a data request occurs from these data request terminal unit, about those data requests, performing attestation based on a predetermined attestation standard -- (1) -- to a data request terminal unit which performed said data request according to a result of the attestation, determining whether transmit the demanded data -- (2) -- always -- or according to a result of the attestation with a data transfer unit which outputs data request history information containing said identifier of the data request terminal unit. A controlling device which acquires said said outputted data request history information, judges whether a data request terminal unit contained in the data request history information by predetermined judging standard is regular, is based on the decision result, and creates or updates criteria of control.

[Claim 12]A medium recording a program for making a computer perform any of claims 1-10, or all or a part of steps of each steps of one statement.
[Claim 13]A medium recording a program for making a computer perform a function of all or a part of means of each means according to claim 11.

[Translation done.]